2020

Hacking for Intelligence Collection in the Fight Against Terrorism: Israeli, Comparative, and International Perspectives

Asaf Lubin
Maurer School of Law - Indiana University, lubina@iu.edu

תקיפות מחשבים למטרות איסוף מודיעין
כחלק מהמאבק בטרור בדין הישראלי, המשווה והבין-לאומי

אסף לובין[1]

הניסיון של המחוקק הישראלי להביא להסדרה מפורשת של סמכויות השב"כ במרחב הקיברנטי משקף מגמה רחבה יותר הניכרת בעולם לעיגון בחקיקה ראשית של הוראות בדבר פעולות פצחנות מצד גופי ביון ומודיעין ורשויות אכיפת חוק למטרות איסוף מודיעין לשם סיכול עבירות חמורות, ובייחוד עבירות טרור אם בעבר היו פעולות מסוג אלה כפופות לנהלים פנימיים ומסווגים, הרי שהדרישה לשקיפות בעידן שלאחר גילויי אדוארד סנודן מחד והשימוש הנרחב בתקיפות מחשב לביצוע פעולות חיפוש וחקירה לסיכול טרור מאידך, מציפים כעת את הדרישה להסמכה מפורשת. במאמר זה אבקש למפות הן את השדה הטכנולוגי והן את השדה המשפטי בכל האמור בתקיפות מחשבים למטרות ריגול ומעקב. יש לשים לב כי המאמר עוסק בעיקר בהיבטי איסוף מידע, ובפעולות פצחנות למטרות אחרות – רק בעקיפין. במאמר זה אבקש לבחון אם התיקון התלוי ועומד לחוק השב"כ, המבקש להקל על השב"כ בביצוע תקיפות מחשב כחלק מהמאבק בטרור, עולה בקנה אחד עם מחויבויותיה הבין-לאומיות של ישראל, ובייחוד לכללים המנהגיים המקיפים את הזכות לפרטיות בדיני זכויות האדם הבין-לאומיים. המאמר נשען גם על בחינתה של חקיקה משווה אגב עיון בדין האמריקאי, האנגלי, הצרפתי והאיטלקי, כדי לעמוד על קנקנם של האיזונים והבלמים המגולמים בשיטות משפט אחרות, וכיצד הם מובחנים מהמנגנון המוצע בדין הישראלי. המאמר חותם בכמה וכמה עקרונות מנחים בהסדרה עתידית של התחום בהקישו מתזכיר חוק סדר הדין הפלילי (סמכויות אכיפה – המצאה, חיפוש, כניסה ותפיסה), התשע"א–2011.

---

[1] ד"ר אסף לובין, מרצה מן החוץ באוניברסיטת ייל, בתר-דוקטורנט במדיניות הגנת סייבר, בית הספר פלצ'ר למשפט ולדיפלומטיה של אוניברסיטת טאפטס, עמית מחקר במרכז ע"ש ברקמן קליין לחקר מדיניות אינטרנט וחברה של אוניברסיטת הרווארד, עמית מחקר בפרויקט חברת המידע של בית הספר למשפטים של אוניברסיטת ייל, חוקר אורח במרכז המחקר ע"ש פדרמן להגנת הסייבר של הפקולטה למשפטים באוניברסיטה העברית בירושלים. על הערות ותובנות מחכימות על טיוטות קודמות של רשימה זו אני מבקש להודות למשתתפי הסדנה בנושא המשפט והמרחב הקיברנטי בהובלת המכון למחקרי חקיקה ולמשפט השוואתי ע"ש הרי ומיכאל סאקר. עוד אבקש להודות לטומאסו פלצ'אטה וליתר עובדי ארגון Privacy International, וכן לאפרת חקאק מוועדת החוקה, חוק ומשפט, על סיוע נקודתי בשאלות הנוגעות ברשימה זאת. אני מבקש להודות לחברי מערכת כתב העת **חוקים** ובייחוד לעורך אהרן טופר על קריאה מעמיקה ומפרה של המאמר.

"All of our exalted technological progress, civilization for that matter, is comparable to an axe in the hand of a pathological criminal"

Albert Einstein, Letter to Heinrich Zangger (1917)

א. הקדמה

"סיימון ידידי, אבי נפטר לפנות בוקר, אנחנו מרוסקים, אני שולח לך פרטים על השבעה, אני מקווה שתוכל להגיע"; "היי, מחוץ לביתך ישנו ואן עם שני אנשים חמושים, צילמתי תמונות תסתכל עליהן ותהיה זהיר"; "שגרירות ארה"ב/ זיהינו בעיה הקשורה בוויזה שלך. אנה סורי במהירת לשגרירות. ראי פרטים"; "אזהרת אמבר/ עזרתך נחוצה באיתור ילד בן 9 אשר נעלם בשכונת מגוריך".[2]

[2] לרשימה המלאה של הודעות הטקסט שנשלחו כחלק מאירועי תקיפת המכשירים במקסיקו ראו: John Scott-Railton et al., *Reckless Exploit, Appendix A: Full Message List*,

ביוני 2017 פרסם מכון המחקר הקנדי, Citizen Lab, הפועל מאוניברסיטת טורונטו, רשימה שכותרתה "חולשה שרירותית". על פי הפרסום, בין אוגוסט 2015 ליולי 2016 נשלחו יותר מ-76 הודעות טקסט (דוגמת אלה המופיעות לעיל) ממספרים לא מזוהים לכמה וכמה עיתונאים, עורכי דין ופעילי זכויות אדם מקסיקנים ובני משפחותיהם. כל הודעות הטקסט כללו קישורים שלחיצה עליהם הייתה מעניקה לרשויות המקסיקניות, כך על פי הנייר, גישה ישירה למכשירים האלקטרוניים של קורבנות המתקפה. עוד נטען כי כלל הקורבנות היו מעורבים בצורה כזאת או אחרת במאבק הציבורי סביב חשדות לשחיתות ולהפרות זכויות אדם ומִנהל תקין בממשל המקסיקני הפדרלי. "אנחנו אויבי העם החדשים", הכריז חואן פרדינאס, מנכ"ל המכון המקסיקני לתחרותיות, ומי שנפל בעצמו קורבן למתקפת ההודעות הדיגיטליות. "הדמוקרטיה בחברה שלנו נשחקה", הוסיף.[3] ביולי 2017 פרסמו ארבעה מהדווחים המנחים של מועצת זכויות האדם של האו"ם קריאה משותפת לממשלת מקסיקו להפסיק לעקוב אחר פעילי זכויות אדם ועיתונאים, לקיים חקירה עצמאית ושקופה על השימוש שנעשה בכלי ריגול ותקיפה לצרכים אלו ולאמץ בחקיקה מנגנוני בקרה אפקטיביים על רשויות הביון והביטחון שמא ינצלו לרעה בשנית את כלי המעקב שברשותם.[4]

THE CITIZEN LAB (Jun. 19, 2017) https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/.

[3] Azam Ahmed & Nicole Perlroth, *Using Texts as Lures, Government Spyware Targets Mexican Journalists and Their Families*, N. Y. Times, (Jun. 19, 2017) https://www.nytimes.com/2017/06/19/world/americas/mexico-spyware-anticrime.html. לקריאה נוספת ראו: גיא אלסטר "תוכנת הריגול הישראלית שמשמשת את מקסיקו למעקב אחר עיתונאים" **וואלה! חדשות** 20.6.2017. http://news.walla.co.il/item/3074732.

[4] חתומים על ההכרזה הדווח המנחה לסיטואציה של מגיני זכויות אדם, הדווח המנחה לזכות לחופש ביטוי ודעה, הדווח המנחה לזכות לפרטיות והדווח וראש קבוצת העבודה להיעלמויות כפויות. ראו: Mexico: UN experts call for an independent and impartial investigation into use of spyware against rights defenders and journalists, UN OFFICE OF THE HIGH COMMISSIONER FOR HUMAN RIGHTS (Jul. 19, 2017), https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=21892.

על פי החשדות, הרשויות במקסיקו השתמשו במערכת לניצול חולשות של חברת NSO Group הישראלית "פגסוס", שאותה רכשו בסכום כולל של כ-80 מיליון דולר. בכתבה שפורסמה בעיתון גלובס ביוני 2017 תוארה המערכת ככזו הפורסת "סוכנים" בלתי נראים ה"מזריקים" את עצמם ללא הרשאה לתוך טלפונים חכמים "ומוצצים מתוכם את תוכני הפונקציות שלהם". לצד זאת מסוגלת פגסוס "להפעיל הקלטות באמצעות מיקרופון, תזרימי תצלומים, איתור גאוגרפי של המכשיר ופונקציות נוספות". כפי שמתאר זאת עומרי לביא, אחד ממייסדי החברה, ממרכז הפיקוד והבקרה שלהם בהרצליה מסוגלים עובדי NSO Group "לספק מידע מודיעיני מתמשך ומדויק ממכשיר טלפון בנאירובי, בסודאן, או בכל מקום אחר בעולם".[5]

מערכת "פגסוס" ופרשת הריגול המקסיקנית מספקות לנו הצצה לעולם דיסטופי שאיננו עוד נחלתם הבלעדית של סופרי מתח, ריגול ומדע בדיוני. היכולת לרכוש בכסף "רוחות רפאים" ולהחדירם לתוך המכשירים האלקטרוניים שבהם כולנו

---

[5] רן דגוני "ממשלת מקסיקו מפעילה תוכנת ריגול ישראלית נגד מתנגדים מבית" **גלובס** (20.6.2017)
https://www.globes.co.il/news/article.aspx?did=1001193261
באפריל 2015 התראיין שלו חוליו, אחד המייסדים האחרים של חברת NSO, לפודקאסט "השבוע". חלק מהריאיון כולל התייחסות לשאלה אם נכון לסווג את מערכת "פגסוס" כמערכת נשק. להלן תמליל הריאיון: "המראיין: זה סוג של נשק בעצם, נכון? ; שלו: אני לא... תראה... ; המראיין: אתה יצואן נשק בעצם אחי... (צחוקים) שלו: כן, זה אני, warlords ; המראיין: תגיד, אתה יצואן נשק? לדעתך נכון להגדיר את זה בתור ייצוא נשק? ; שלו: אה, לא, כי זה לא הורג. אני חושב שנשק תפקידו בסוף להרוג, ואני מאוד סולד מזה. אני חושב שאנחנו ממש לא בתחום של הנשק. אני חושב שאנחנו בדיוק ההיפך. אומנם זה נקרא סייבר התקפי, אבל תפקידנו בסוף זה לבוא ולהגן. בכל המקומות – ואני כמובן לא אפרט – שמכרנו את המערכות שלנו, הדבר הזה מציל, באמת לא עם פאתוס, מציל באמת יום יום חיים של אנשים ; המראיין: בגלל שהוא מונע פיגועים? ; שלו: הוא מונע פיגועים, הוא עוזר לתפוס אנשים, למצוא מיקומים של אנשים שנחטפו, הא עוזר למנוע הברחות מאוד מאוד גדולות של סמים בכל מיני מדינות, הוא עוזר למנוע הפיכות ; המראיין: אתם בעצם חברה שמספקת כלים למודיעין, לממשלות? ; שלו: בסוף, NSO היא חברה טכנולוגית. בסדר? היא חברה שמפתחת טכנולוגיה. היא לא עושה שום פעולה בעצמה. הטכנולוגיות שאנחנו מפתחים, אנחנו מוכרים אותן לממשלות בעולם, והם משתמשים בטכנולוגיות האלה כדי בעצם לשמור על השלטון התקין, שזה אומר למנוע פשיעה ולמנוע טרור ולמנוע הפרעה לשלטון". ראו: עידן לנדאו "למנוע הפרעה לשלטון": על קורבנות הסייבר הישראלי, ועל עיוורונו" לא למות טיפש: הבלוג של עידן לנדו (29.7.2017)
https://idanlandau.com/2017/07/29/preventing-disturbance-to-to-power-israeli-cyber/
לנדאו מתמלל קטע מריאיון (בדקות 52:7–31:9) שנעשה כחלק מפודקאסט "השבוע", פרק 29, הזמין בקישור: http://www.shavua.net/29.

משתמשים תדיר, מקימה עלינו מציאות המחייבת בחינה מחדש של גבולות הכוח של שירותי ביון ואכיפה. התפתחותה של "חברת המידע" הביאה עימה שינויים מהותיים בצומת היחסים שבין טכנולוגיה, חברה ורגולציה.

לפני שלוש-עשרה שנים הרהיב השופט חשין לתאר את שינויי הטכנולוגיה שהביאה עימה רשת האינטרנט במונחים מעולמות הגֵאולוגיה והזואולוגיה:

> "כך בשינויי אבולוציה. לא כך בשינויי רבולוציה. ברעידות-אדמה ההורסות ערים ומשקעות אותן במעמקי-ים. וכיום מצויים אנו בשינויי טכנולוגיה של רבולוציה. שכן המחשב – ועימו האינטרנט – אינם אך מוטציה של צורות חיים קודמות שהכרנו ואשר בְּיַּתְנוּ בשיטת המשפט. חיים חדשים הם, והילוכם אין הוא כהילוך צורות החיים שהורגלנו לחיות בחברתן... צורות חיים חדשות אלו של המחשב והאינטרנט טרם ירדנו לחיקורן, טרם הגענו אל תחתית הבור. נקישה אחת בירושלים, ואתה בתל אביב; נקישה שניה, ואתה באוסטרליה; נקישה שלישית – המערכת מתמרדת, והכל נמחק כלא היה. החילונו נעים במהירות האור בעוד שגופנו בכרכרה וזרימת מחשבתנו כמהירות הכרכרה".[6]

אם המחשב והאינטרנט היוו את רעידת האדמה הראשית, הרי שהמעבר ל"נְתוּנֵי עָתֵק" (Big Data)[7] וטכנולוגיות "מִרְשָׁתֶת הַדְּבָרִים" (Internet Of Things)[8] מגלמים בתורם את הרעידות העוקבות. שילובן של טכנולוגיות האינטרנט והאינטרנט האלחוטי עם מחשוב ענן, מערכות משובצות-מחשב ומערכות מיקרו אלקטרו-מכניות אפשרו בעשור האחרון את פיתוחו של שוק חדש של מוצרים "חכמים" הצומח לו

---

[6] דנ"א 6407/01 **ערוצי זהב ושות' נ' Tele Event Ltd**, פ"ד נח(6) 6, 27 (2004).

[7] מונח המתייחס לאיסוף נתונים בכמויות עצומות, המגיעים ממקורות שונים ומגוונים, באיכויות שונות ובמבני נתונים שונים. איסוף זה מאפשר שורה של ניתוחים סטטיסטיים תוך שימוש בכלים אלגוריתמיים. לקריאה נוספת ראו: עופר דודזדה ואמיר סנדץ, **ביג דאטא- כלים מעשיים לניתוח בסיסי נתונים** (2014).

[8] מִרְשָׁתֶת הַדְּבָרִים הינה רשת הכוללת שורה של טכנולוגיות משובצות אלקטרוניקה, תכנה וחיישנים המאפשרים קישוריות אינטרנטית. דרך כך טכנולוגיות אלה מאפשרות יכולות איסוף והחלפת מיעד וכן עשויות להוביל לאוטומיזציה בתחומים שונים. לקריאה נוספת ראו: רועי צוזנה, **השולטים בעתיד: הון-שלטון טכנולוגיה תקווה** חלק ראשון "האינטרנט של הדברים" (2017).

בקצב מואץ. מהמכשיר הנייד החכם עברנו לצעצועים החכמים, ומהם לרכב החכם ולציוד הרפואי וההנדסי החכמים, ועברנו עוד למכשור האלקטרוני החכם (כמו המקרר החכם או תנור המיקרוגל החכם)[9] ועד לעיר החכמה על תשתיותיה החכמות – ומהי אותה "חוכמה" נסתרת? הרי היא היכולת לאסוף, לחבר, לנתח ולשתף במידע ברציפות ובהיעדר אמצעיות. על פי הערכות, בסוף שנת 2020 יגיע מספר ההתקנים המחוברים בעולם לכ-26 מיליארד, ועד לשנת 2025 שווי השוק הגלובלי של מוצרים אלה צפוי לטפס עד לכדי 620 מיליארד דולרים.[10] ועם זאת שמוצרים אלו מבטיחים אין-ספור הזדמנויות להעצמתה ולהתפתחותה של החברה האנושית, הם מקפלים בתוכם איומי ביטחון ואתגרים להגנת המידע.[11] ארגון Consumers International, לדוגמה, קבע בנייר מדיניות מ-2016 כי טכנולוגיות מרשתת הדברים מייצרות לפצָחָנִים (האקרים) "יותר חולשות ברות-ניצול ביותר סביבות עבודה, ולאור הגידול בקישוריות שבין המוצרים השונים, ובינם לבין מערכות נוספות, הרי שגם יותר הזדמנויות לתקיפה ופוטנציאל נזק חמור יותר".[12] בתווך הזה נכנסים גופי ביון ורשויות אכיפת חוק שמחד מבקשים להגן על הציבור מפני הסכנות הגלומות בעבירות סייבר המנצלות פרצות מסוג אלה, ומאידך מעוניינים לנצל בעצמם את אותן הפרצות כדי שיוכלו לעקוב באפקטיביות רבה יותר יותר ובהרמטיות רבה יותר אחר עבריינים פוטנציאליים ואף לנטרל מבעוד מועד איומים שונים על ביטחון הפנים של המדינה, דוגמת טרור, ריגול זר ופשיעה מאורגנת.

---

[9] זכורה במיוחד הצהרתה של קליאן קונווי, היועצת הבכירה של נשיא ארה"ב דונלד טראמפ, לפיה ייתכן שימוש במיקרוגלים למטרות ריגול ומעקב. דבריה זכו ללעג מוצדק, שכן גם אם תיתכן חדירה למכשירי מיקרוגל, ספק אם במידע הנאסף באמצעותם ייתכן ערך מודיעיני ממשי. יחד עם זאת דבריה נותנים ביטוי לתחושות עומק בציבוריות בדבר אי-הוודאות באשר להיקפה של "חברת המעקב" וגבולות כוחה. לקריאה נוספת ראו: Lily Hay Newman, *No, Microwave Ovens Cannot Spy on You – For Lots of Reasons*, WIRED MAGAZINE (Mar. 13, 2017) https://www.wired.com/2017/03/kellyanne-conway-microwave-spying/.

[10] ראו: עומר שוברט "האינטרנט של הדברים נמצא בשלב 1.0" **דה מרקר** 29.4.2014 https://www.themarker.com/technation/1.2307339.

[11] לקריאה נוספת על אודות הסביבה הטכנולוגית הכלכלית והמשפטית הקשורה במוצרי מרשתת הדברים ראו: ROLF H. WEBER & ROMANA WEBER, INTERNET OF THINGS: LEGAL PERSPECTIVE (2010).

[12] ראו: CONSUMERS INTERNATIONAL, THE INTERNET OF THINGS AND CHALLENGES FOR CONSUMER PROTECTION 32 (2016).

לא מפתיע אפוא כי בשנים האחרונות ניכרת בעולם מגמה רחבה לעיגון בחקיקה ראשית של הוראות בדבר פעולות פצחנות מצד גופי ביון ומודיעין למטרות סיכול עבירות חמורות, ובייחוד עבירות טרור. אם בעבר היו פעולות מסוג אלה כפופות לנהלים פנימיים ומסווגים, הרי שהדרישה לשקיפות בעידן שלאחר גילויי אדוארד סנודאן מחד, והשימוש הנרחב בתקיפות מחשב לביצוע פעולות חיפוש וחקירה לסיכול טרור מאידך, מציפים כעת את הדרישה להסמכה מפורשת.[13] רגולציה זו מבקשת לקבוע את נקודת האיזון שבין הצורך להעניק לרשויות המדינה את הכלים לאכיפה אפקטיבית של החוק בעידן הדיגיטלי בתוך כדי שמירה על חירויות הפרט ועל שלמות מערכי התקשורת שבהם אנו תלויים. פרשת הריגול המקסיקנית, כפי שתוארה לעיל, היא אפוא דוגמה למקרה קיצון שבו פעולות פצחנות, מצד רשויות שלטוניות, מבוצעות ללא הסדרה בחקיקה וללא פיקוח דמוקרטי מספק עליהן.[14]

מגמת ההסדרה מוצאת את ביטויה גם בדין הישראלי, בדמות תיקון תלוי ועומד לחוק השב"כ אשר מבקש לעגן את סמכות השירות לבצע תקיפות פצחנות אגב השוואת ההסדרים הנוגעים לפעולות אלה לאלה הקבועים בחוק האזנת סתר, התשל"ט–1979, ובראשם הסמכות לביצוע התקיפות ללא צו בית משפט.[15] במאמר זה

---

[13] לקריאה נוספת אודות מגמות אלה בעולם ראו: Policy Department C- Citizens Rights and Constitutional Affairs, Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, Study for the LIBE Committee, PE 583.137 (2017) http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf (להלן: דוח המחלקה למדיניות זכויות אזרחים ויחסים חוקתיים).

[14] על היעדר חקיקה המסדירה פעולות פצחנות בדין המקסיקני, בניגוד לעקרון החוקיות המגולם בדיני זכויות האדם הבין-לאומיים, ראו: Privacy International, *International Human Rights Implications of Reported Mexican Government Hacking Targeting Journalists and Human Rights Defenders*, 12-15 (2017), https://medium.com/@privacyint/letter-to-mexican-government-on-the-reported-hacking-of-civil-society-e531808dd9b2

(שם נטען כי פעולות פצחנות מצד הממשל המקסיקני משוללות כל בסיס משפטי לפי הדין המקסיקני המקומי, שכן המסגרת המשפטית הקיימת עוסקת רק בהאזנות סתר ואינה מגלמת את האיזונים הייחודיים לפעולות פצחנות. מכל מקום נקבע עוד בדוח כי פעולות הפצחנות המקסיקניות, כפי שפורסמו על ידי Citizen Lab, אף אינם עולים בקנה אחד עם המסגרת המשפטית הנוגעת להאזנות סתר).

[15] סעיף 131 להצעת חוק המאבק בטרור, התשע"א–2011, ה"ח 611.

אני מבקש לבחון את לשון התיקון המוצע לחוק בראי הדין המשווה והבין-לאומי ולהציע שורת המלצות למחוקק בטרם יאושר התיקון.

למאמר שלושה חלקים מרכזיים: חלק ב עניינו השדה הטכנולוגי, ובו אני מבקש להציע "מורה נבוכים" לתופעת הפצחנות ולשיקולים המנחים רשויות אכיפת חוק בשימוש בכלים אלו. דגש מיוחד מושם בחלק זה על מרכיביהן השונים של נוֹזְקוֹת מסוג רוֹגְלָה ועל צורות השימוש בה מצד גופי ביון וביטחון. חלק ג מתמקד בשדה המשפטי, והוא עיקרו של מאמר זה. החלק מורכב משלושה תתי-חלקים: הראשון בוחן את הדין הישראלי בדגש על המסגרת המשפטית המגולמת בחוק האזנת סתר ובחוק השב"כ ובתיקון העומד בפני ועדת החוקה, חוק ומשפט של הכנסת; השני דן בפרשנויות השונות הקבועות במשפט הבין-לאומי, בדגש על דיני זכויות האדם הבין-לאומיים, בכל האמור בחובות המוטלות על מדינות סביב שימוש בכלי פצחנות; לבסוף נסקר את הדין הקיים כיום סיקור השוואתי, בדגש על האיזונים והבלמים המגולמים בו, בארבע מדינות שונות. שתי מדינות מהמשפט המקובל (ארצות הברית ואנגלייה) ושתי מדינות מהמשפט הקונטיננטלי (צרפת ואיטליה). חלק ד חותם נייר זה ומציג עקרונות מנחים להסדרה למחוקק בראי הדין המשווה והדין הבין-לאומי, אשר תקוותי כי יסייעו בהעשרת השיח סביב התיקון אשר צפוי לעלות בדיוני חברי הכנסת העשרים ואחת.

יובהר כי עיקרו של נייר זה בפעולות פצחנות למטרות איסוף מודיעין המבוצעות מתוך שטחי המדינה נגד מטרות הפועלות בשטחה. בכך מבקש הנייר להתמקד בפעולות לאיסוף מודיעין פנים (domestic surveillance) ולא לאיסוף מודיעין חוץ (foreign surveillance), לפי המנדט הייחודי של השב"כ כגוף ש"מופקד על שמירת ביטחון המדינה, סדרי המשטר הדמוקרטי ומוסדותיו, מפני איומי טרור, חבלה, חתרנות, ריגול וחשיפת סודות מדינה".[16] עם זאת הן בבחינת הדין המשווה והן בשלב ההמלצות מובאת התייחסות, גם אם בקצרה, להסדרתן של פעולות פצחנות למטרות איסוף מודיעין חוץ. עוד יובהר כי הגם שהנייר מתמקד בפעולות של איסוף מודיעין, תהיה התייחסות גם לפעולות פצחנות אחרות, הכוללות מניפולציה על המידע, מודיפיקציה של המידע, הצפנת המידע או הגבלת גישה אליו, וכן מחיקה של

[16] סעיף 7(א) לחוק שירות הביטחון הכללי, התשס"ב–2002.

המידע מהמכשיר המותקף.[17] עם זאת גם הדיון הזה ייעשה במשורה, שכן הוא חוצה את גבולות נייר זה.

ב. מיפוי השדה הטכנולוגי

1. כובעים לבנים ופינות חשוכות

בבסיסה של כל פעולת פצחנות קיימת "התוכנה הזדונית" (malware) או הנוזקה. דוגמה לנוזקה כזו היא זו שנמצאה במתקפת Wannacry שהחלה ב-12 במאי 2017 וזכתה לתואר מתקפת הסייבר החמורה בהיסטוריה. המתקפה השתמשה בנוזקת כופר (ransomware) שניצלה פרצת אבטחה במערכת ההפעלה windows. אומנם פרצה זו זוהתה ונחסמה בעדכון גרסה שהוציאה חברת מייקרוסופט, אך מיליוני מחשבים ברחבי העולם טרם עדכנו את גרסתם, ולכן היו חשופים לתקיפה.[18] הנוזקה תוכנתה להצפין את המסמכים השמורים במחשב המודבק. התוקפים, אשר על פי חלק מההערכות היו צפון-קוריאנים,[19] דרשו 300 דולר במטבע הווירטואלי ביטקוין, בטרם יסכימו לשחרר את המסמכים שבמחשב מההצפנה. המחשב הראשון נדבק באמצעות

---

[17] מאמר זה לא דן בתזכיר חוק הגנת הסייבר ומערך הסייבר הלאומי, התשע"ח–2018. יובהר כי מכוח התזכיר, אם יאומץ כחוק, תקום למערך הסייבר הסמכות לאיסוף מידע לשם איתור תקיפות סייבר (לרבות תקיפות מצד ארגוני טרור) וטיפול בהן. לדעת המערך "יש הבדל עקרוני בין הפרק האופרטיבי (בתזכיר בדבר סמכויות איסוף) לבין חקיקה אחרת העוסקת ומסדירה את הסמכויות של רשויות המדינה בכל הנוגע לפעילות הקשורה למידע המצוי במחשבים ובתקשורת" (שם, בעמ' 6–7). בגבולות מאמר זה אני נאלץ להשאיר טענה זו בצריך עיון.

[18] החולשה שאותרה הייתה בפרוטוקול SMB (Server Message Block), אשר מאפשר גישה משותפת אל קבצים, מדפסות ותקשורת בין מחשבים ברשת. מייקרוסופט פרסמה את טלאי האבטחה הסוגר את הפרצה במארס 2017 כחלק מ-Security Bulletin MS17-010. לקריאה נוספת ראו: Ali Islam, et. al., *SMB Exploited: WannaCry Use of "EternalBlue"*, FIREEYE (May. 26, 2017) https://www.fireeye.com/blog/threat-research/2017/05/smb-exploited-wannacry-use-of-eternalblue.html (להלן: אלי אסלאם ואח' "SMB Exploited").

[19] ראו: Danny Palmer, *North Korea carried out the WannaCry ransomware attack, say security services*, ZDNET (Jun. 16, 2017) https://www.zdnet.com/article/wannacry-ransomware-attack-carried-out-by-north-korea-say-security-services/

דוא"ל פשוט, אך מרגע הדבקתו שכפלה את עצמה הנוזקה כתולעת והדביקה את כל המחשבים הפגיעים אשר היו מחוברים לאותו המחשב ברשת פנימית. בכך גרמה הנוזקה להשבתה של יותר מ-300,000 מחשבים ב-150 מדינות (לרבות בבתי חולים, חברות תקשורת, חברות רכבות ובנקים).[20]

מתקפת Wannacry עלתה לכותרות לא רק בגלל הנזק הכלכלי העצום שגרמה, אלא גם בשל העובדה כי כלי התקיפה, הנוזקה, נכתבה בידי עובדי הסוכנות לביטחון לאומי, ה-NSA, סוכנות ביון ממשלתית של ארצות הברית האחראית לאיסוף ולניתוח מודיעין אותות (Signal Intelligence או SIGINT). בעוד שהסוכנות זיהתה את פרצת האבטחה במערכת windows. היא בחרה שלא לחשוף את פרטיה למייקרוסופט, ובמקום זאת פיתחה את הנוזקה בהתבסס על הפגם. באפריל 2017 הדליפה קבוצת פצחנים המכנים עצמם "מתווכי הצללים" (Shadow Brokers) לרשת כלי פריצה וחולשות שגנבו מה-NSA. אחת מהחולשות כונתה "הכחול-הנצחי" (EternalBlue), והיא החולשה שבה השתמשו תוקפי Wannacry חודש לאחר מכן.[21]

הדיכוטומיה המקובלת בהקשרן של טכנולוגיות ריגול ומעקב עוסקת באיזון שבין פרטיות ובין ביטחון (privacy vs. security), בין הגנה על חירויות הפרט לבין הגנה על הפרט.[22] מגדילים לתאר זאת צוות הכותבים של הסדנה הרב-תחומית במשפט וטכנולוגיה בפקולטה למשפטים באוניברסיטת חיפה (להלן: "עבודת מחקר: לוחמה בטרור בזירת המידע"). הכותבים מציינים כי הזכות לשמירה על הסדר הציבורי "מקימה את הצידוק המוסרי לקיומן של מערכות סיכול ואכיפה" לרבות מערכות ריגול והאזנה. עם זאת מול הזכות הכללית לביטחון עומדות זכויות הפרט לרבות הזכות לפרטיות, לחופש ביטוי, לחופש דעה ולהתאגדות. הניסיון לאזן בין זכויות

---

[20] ראו: אמיתי זיו "כל מה שרציתם לדעת על מתקפת הסייבר הגדולה בהיסטוריה" **דה מרקר** (13.5.2017) https://www.themarker.com/wallstreet/1.4088541.

[21] שם; אלי אסלאם ואח' "SMB Exploited", לעיל ה"ש 18.

[22] ראו לדוגמה: JULIA ANGWIN, DRAGNET NATION: A QUEST FOR PRIVACY, SECURITY, AND FREEDOM IN A WORLD OF RELENTLESS SURVEILLANCE (2014); Adam D Moore, *Privacy, Security, and Government Surveillance: Wikileaks and the New Accountability*, 25(2) PUB. AFF. Q. 141 (2011).

מתנגשות אלה מעורר מצבים מורכבים. כך למשל שואלים הכותבים: "האם יש לתת למדינה את האפשרות לצותת לכל שיחה או מידע העובר ברשת ללא כל בקרה? או שמא יש להגבילה למקרים מיוחדים בלבד?"[23]

הנשיא ברק תיאר אף הוא את המתח המקובל בפעולות ריגול בין פרטיות לביטחון, בעניין **נחמיאס**, שם קבע בהקשרן של האזנות סתר:

> "האזנת סתר היא התערבות חריפה בזכותו של אדם להיות עם עצמו. היא מהווה חדירה קשה לפרטיותו של האדם. היא שוללת מהאדם את מנוחת נפשו, את ביטחונו בחופש רצונו. היא הופכת את מבצרו לכלאו. עם זאת הזכות לפרטיות אינה מוחלטת. ניתן לפגוע בה לשם מניעת עבירות, אשר סופן הגנה על הפרטיות של אחרים, ועל כבודם וחירותם".[24]

אלא שפעולות פצחנות אינן כשאר טכניקות הריגול, שכן בבסיסן קיים הצורך בניצול חולשות במערכות תקשורת ומחשוב מתוך כוונה לפעול בחשאי ומרחוק מתוכן ללא הסכמתו או ידיעתו של המשתמש, הבעלים של המערכת, או החברה היצרנית. זיהוין, אגירתן וניצולן של חולשות אלה יוצרים עתה מתח חדש, אשר פרשת Wannacry מדגימה היטב. לא עוד המתח הרגיל שבין הגנה על חירויות הפרט להגנת הפרט כי אם מתח חדש בין הגנת הפרט להגנת הפרט (security vs. security). הדגש מושם בעיקר על אגירתן של חולשות אפס-ימים (Zero-day Vulnerabilities), קרי חולשות שמאז יום פרסומן עברו אפס-ימים (קרי טרם נחשפו ליצרן ופורסמו לציבור).[25]

---

[23] א' אינהורן ואח', **לוחמה בטרור בזירת המידע** (בעריכת נ' אלקין-קורן ומ' בירנהק, חיפה: המרכז למשפט וטכנולוגיה, אוניברסיטת חיפה, 2002), עמ' 65.

[24] ע"פ 1302/92 **מדינת ישראל נ' נחמיאס**, פ"ד מט (3) 309, 312 (1995) (להלן: עניין **נחמיאס**).

[25] להגדרה של פרצת אבטחה מסוג "אפס-ימים" ראו: Steven M. Bellovin et. al., *Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet*, 12(1) NORTHWESTERN J. TECH. & INTELL. PROP. 1, 23 (2014) ("A zero-day is a vulnerability discovered and exploited prior to public awareness or disclosure to

בהשאלה ממערבוני הספגטי של שנות השישים הפרקטיקה מבחינה בין שלושה סוגים של פצחנים: **חובשי הכובע השחור** (אשר המוטיבציה הראשית שלהם מפעולת הפצחנות היא השגת תועלת אישית, כלכלית או אחרת, ואשר עסוקים בזיהוי חולשות ופיתוח נוצלות כדי לגנוב, לשנות ולהרוס מידע); **חובשי הכובע הלבן** (הפועלים בהרשאה ממפתחי המערכות ומתוך מטרה לאתר מבעוד מועד פרצות ולפתח להן טלאי אבטחה מתאימים. לעיתים מכנים את אלה "הפצחנים האתיים"); **חובשי הכובע האפור** (אלה מחזיקים במוטיבציות משתנות. הגם שמטרתם אינה זדונית, הם פועלים ללא הרשאה ובניגוד לחוק, וכאשר הם מאתרים חולשות לרוב יפנו למפתח בדרישה לסכום סמלי (Bounty Hunting) או לחלופין יפרסמו את החולשה באינטרנט כאקט של עשיית דין עצמי (Vigilantism).[26]

ארגוני ביון וביטחון רואים עצמם בטבעיות כחובשי הכובע הלבן, כמי שאמונים על שמירת החוק והסדר ואכיפתם. אלא ששיטות העבודה שלהם זהות לאלה של חובשי הכובע השחור: פעילות במחשכים, ללא ידיעת המפתחים, ומתוך כוונה

---

the vendor. Zero-days are frequently sold in the vulnerabilities market. The vendor and the public often only become aware of a zero-day after a system compromise" (להלן: בלובין ואח', "פצחנות חוקית"). ככלל מדובר בחולשה שהיצרן טרם נחשף אליה, ולפיכך טרם פיתחו לה "טלאי" (patch) תיקון לתוכנה שיטפל בחולשה. לפיכך חולשות אלה הן היקרות ביותר ובעלות פוטנציאל הנזק הרב ביותר.

[26] עוד על אודות ההבחנה בין שלוש הקטגוריות ראו: Nadia Kovacs, *What is the Difference Between Black, White and Grey Hat Hackers?*, NORTON PROTECTION BLOG (Apr. 17, 2015), https://us.norton.com/internetsecurity-emerging-threats-what-is-the-difference-between-black-white-and-grey-hat-hackers.html; עוד ראו: Ellen Nakashima, *FBI paid Professional Hackers One-Time Fee to Crack San Bernardino iPhone*, WASH. POST (Apr. 12, 2016), https://www.washingtonpost.com/world/national-security/fbi-paid-professional-hackers-one-time-fee-to-crack-san-bernardino-iphone/2016/04/12/5397814a-00de-11e6-9d36-33d198ea26c5_story.html?utm_term=.b8aaf2be6964. לקריאה נוספת על הקטלוג של פצחנים על בסיס ה"מניע" לפעילותם לעומת אפשרויות קטלוג נוספות, לרבות הסיכון שבהתמכרות לקטלוגים מסוג אלו, ראו: THOMAS J. HOLT & BERNADETTE H. SCHELL, HACKERS AND HACKING, 17-26 (2013). לקריאה נוספת אודות הדין החל על קבוצות פצחנים אלו ראו: Ido Kilovaty, *Freedom to Hack*, 80(3) OHIO ST. L.J. 455 (2019).

לנצל חולשות לאיסוף, לשינוי ולהריסת מידע. הקושי המיוחד במציאות המבוזרת שמתווה רשת האינטרנט, ושלפיה פועלים אותם הארגונים, היא שאגירה של חולשות שכאלה ופיתוחן של טכנולוגיות התקפיות סופם כי ימצאו דרכם לידיהם של פצחנים זדוניים. אקדח שיופיע במערכה הראשונה יירה במערכה השלישית, והיורה לא יהיה בהכרח שריף העיירה. הגדיל לתאר זאת מייקל היידן, לשעבר ראש ה-NSA, אשר טען כי אנו עדים לגידול בהצטיידות בטכנולוגיות סייבר התקפיות, שבעבר היו בבעלות בלעדית של מדינות, מצד ארגוני טרור, שחקנים פליליים והאקטיביסטים (Hacktivists). "גם אלה בעלי יכולות מוגבלות, יכולים כעת לפתח או לרכוש כלים ונשקים שבעבר חשבנו אותם כיקרים ואקסלוסיביים", מבהיר היידן.[27]

דרך טובה להבין את עולם הגנת הסייבר בעידן האינטרנט היא באמצעות "עקרון פארק היורה" שתבע ברט קאופמן מהאיגוד האמריקאי לחירויות אזרחיות. פרוליפרציה באגירת חולשות וטכנולוגיות התקפיות ובשימוש בהן מעצימה את הסיכון כי אחת מהן תדלוף (כשם שהדינוזאורים מצליחים להשתחרר מהפארק וגורמים לנזק רב בכל פרק מסדרת הסרטים המפורסמת חרף מנגנוני השליטה והבקרה המפוארים של הפארק המתוארים תמיד בהרחבה בתחילת כל סרט).[28]

---

[27] ראו: Nicole Perlroth, *Hacking for Security, and Getting Paid for It*, N. Y. Times (Oct. 14, 2015), https://bits.blogs.nytimes.com/2015/10/14/hacking-for-security-and-getting-paid-for-it/.

[28] ראו: Brett Max Kaufman, *Encryption Backdoors, Vault 7, and the Jurassic Park Rule of Internet Security*, JUST SECURITY (Mar. 10, 2017), https://www.justsecurity.org/38727/encryption-backdoors-vault-7-jurassic-park-rule-internet-security/.

עוד ראו: בלובין ואח', "פצחנות חוקית", לעיל ה"ש 25, בעמ' 47.

("As we know from other situations, whether rare diseases or the effect of cold weather on shuttle O-rings, a rare side effect is more likely to appear when working with a large population sample. The danger of proliferation means each use of an exploit, even if it has previously run successfully, increases the risk that the exploit will escape the targeted device. This introduces a serious wrinkle in the use of vulnerabilities, one that law enforcement must address". החוקרים ממשיכים עוד לתאר שתי סכנות ביטחון נוספות משימוש מופרז בפרצות אבטחה וטכנולוגיות התקפיות: (1) הסכנה של איסוף מוגזם (overcollection), לרבות הסיכון לאיסוף נרחב של מידע אגבי (collateral data); (2) הסכנה שהנוזקה תגרום נזקים לא צפויים ולא רצויים במערכת המותקפת ובמערכות הקשורות אליה).

לשיח מורכב זה יש להוסיף את תופעת ה"החשכה" (Going Dark). הגם שניצניה של התופעה במלחמות הקריפטוגרפיה של שנות התשעים,[29] הרי שהגיעה למלוא בשלותה בשנים האחרונות. עיקרו של מונח זה בפיתוחים טכנולוגיים אשר מקשים את יכולתם של גופי ביון ואכיפת חוק לקבל גישה למידע הנחוץ כחלק מפעילותם השוטפת. שינויים בארכיטקטורת מערכות תקשוב ובטכנולוגיות תקשורת ובאופן מתן שירותי אפליקציה, בייחוד ההטמעה הנרחבת של הצפנה, בדגש על הצפנת קצה-לקצה (end-to-end), מקימות ביתר שאת את אתגר ה"החשכה",[30] קרי את הסיכון שגופי אכיפת חוק לא יוכלו לאסוף מודיעין נגד מפירי חוק וגורמי טרור וריגול אשר ישמישו כלים מוצפנים אלו. נער הפוסטר של התופעה הוא ג'יימס קומי, לשעבר ראש לשכת החקירות הפדרלית, ה-FBI. הוא שנשא את הנאום המכונן, באוקטובר 2014 במכון ברוקינגס, שבו תיאר את עולם הטכנולוגיה, עולם הפרטיות ועולם

---

[29] לקריאה על מלחמות הקריפטוגרפיה של שנות התשעים ראו: Danielle Kehl et. al., *Doomed to Repeat History: Lessons from the Crypto Wars of the 1990s*, NEW AMERICA (Jun. 2015), https://static.newamerica.org/attachments/3407-doomed-to-repeat-history-lessons-from-the-crypto-wars-of-the-1990s/Crypto%20Wars_ReDo.7cb491837ac541709797bdf868d37f52.pdf.

[30] המרכז ע"ש ברקמן קליין לחקר מדיניות אינטרנט וחברה באוניברסיטת הרווארד תיאר את השפעת חדירתן של טכנולוגיות ההצפנה על תופעת ה"החשכה" כך: "While the going dark problem encompasses a range of architectural changes that impede government access, the adoption of encryption of data at rest, and end-to-end encryption in some common communications applications, by companies has become a focal point in the current debate, particularly those in which service providers do not have access to the keys. For example, *end-to-end* encryption is being used to describe scenarios in which information is being encrypted at the end points of a communication channel, and only the original sender and intended recipient possess the keys necessary to decrypt the message. In other words, the information is (in theory, and as advertised) not capable of being read by anyone who sees in traverse a network between the sender and receiver, including an intermediary service provider, such as Apple. Similarly, *device* encryption – in which the keys exist only on locked devices – prevents the contents from being read by anyone who does not possess the keys". ראו: BERKMAN CENTER FOR INTERNET AND SOCIETY AT HARVARD UNIVERSITY, DON'T PANIC: MAKING PROGRESS ON THE "GOING DARK" DEBATE, 4 (2016) (להלן: דוח מרכז ברקמן).

הביטחון הציבורי כשלושה עולמות הנעים זה אל עבר זה על מסלול התנגשות חזיתי. בבסיס הטיעון של קומי היו כלי ההצפנה המסייעים לשיטתו לעבריינים להתחמק מעונש.[31]

הגידול בשימוש בכלי הצפנה דוחף את גופי הביון והאכיפה לרכוש ולפתח כלי תקיפה ופצחנות כדרך חלופית להשגת גישה למידע.[32] המאבק המשפטי הממושך של ה-FBI נגד חברת אפל כדי שזו תסייע למדינה לפרוץ את ההצפנה של מכשיר האייפון של מבצע הפיגוע בסן ברנדינו, הסתיים ב-2016 רק לאחר שלשכת החקירות הפדרלית שילמה, כך על פי הערכות, 900 אלף דולר לחברת סלברייט הישראלית שתפרוץ בעבורם את המכשיר.[33] המרכז ע"ש ברקמן קליין לחקר מדיניות אינטרנט וחברה באוניברסיטת הרווארד מעריך עוד כי החדירה של טכנולוגיות מרשתת הדברים לתוך

---

[31] הנאום המלא זמין באתר האינטרנט של ה-FBI. ראו: James B. Comey, *Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?*, FBI NEWS (Oct. 16, 2014), https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course

Unfortunately, the law hasn't kept pace with technology, and this disconnect had ") created a significant public safety problem; We call it "Going Dark" and what it means is this: Those charged with protecting our people aren't always able to access the evidence we need to prosecute crime and prevent terrorism even with lawful authority. We have the legal authority to intercept and access communications and information pursuant to court order, but we often lack the technical ability to do so. We face two overlapping challenges. The first concerns real-time court-ordered interception of what we call "data in motion," such as phone calls, e-mail, and live chat sessions. The second challenge concerns court-ordered access to data stored on our devices, such as e-mail, text messages, photos, and videos – or what we call "data at rest." And both real-time communication and stored data are increasingly encrypted").

[32] ראו לדוגמה: Andrew Keane Woods, *Encryption Substitutes*, HOOVER INSTITUTION ESSAY (Jul. 18, 2017), https://www.hoover.org/research/encryption-substitutes .

(בו מתאר פרופסור וודס כיצד "הפרעה לציוד" (equipment interference), שם נרדף לפעולת פצחנות, היא חלופה אפשרית במקרים של הצפנה).

[33] אילן גלר "ה-FBI שילם לחברה ישראלית 900 אלף דולר לפרוץ לאייפון אחד" **וואלה! חדשות** (11.5.2017) https://www.globes.co.il/news/article.aspx?did=1001188240.

המרחב הפרטי והציבורי רק צפויה לדחוף את המדינה להגדיל יותר את יכולת הפצחנות שלה סביב טכנולוגיות אלה.[34]

סיכומם של דברים, על רקע התפתחותן של טכנולוגיות מעצימות-פרטיות דוגמת טכנולוגיות הצפנה ואנונימיזציה, ובשל השימוש הגובר של גורמים עוינים בערוצי תקשורת אשר נשענים על טכנולוגיות אלה, גדל הצורך של גורמי ביון ואכיפת חוק בזיהוי חולשות, בדגש על חולשות אפס-ימים ופיתוח כלי פצחנות. אלא שאליה וקוץ בה. קיים פרדוקס, ולפיו פיתוחם של כלים אלה ואגירתם עלולה להקים בעצמה סכנות לביטחון המידע ולמערכות שבהן אנו משתמשים, ומהווה פרצה הקוראת לגנב אשר עלולה להוביל לפשעים חדשים. פרופ׳ פישר-הובנר מזהה חמישה אספקטים שונים של חברת המידע הגלובלית שיש לנסות ולהגן עליהם בצל השימוש המוגבר בכלי פצחנות מצד גופי ביון ואכיפת חוק: (1) חסיון המידע (confidentiality) – מניעת חדירה לא מאושרת או פרסום לא רצוי של מידע ונתונים; (2) שלמות המידע (integrity) – הבטחת העובדה כי כל הנתונים השמורים במערכת הם ייצוג סמנטי ופיזי מלא ונכון של האינפורמציה, וכי מערכות ומשאבי עיבוד נתונים ממשיכים לבצע פעולות עיבוד רצויות וכשרות; (3) זמינות המידע (availability) – מניעת עיכובים לא מאושרים בשחרור מידע או משאבים; (4) שימושיות המערכות (functionality) – המערכות ממשיכות למלא את כל הפונקציות המגולמות בהן כנדרש; (5) מהימנות המערכות (reliability) – כלל הפונקציות המבוצעות על המערכת מביאות לתוצאות אחידות ללא תלות בנסיבות.[35]

2. על נוזקות ורוגלות

[34] ראו: דו״ח מרכז ברקמן, לעיל ה״ש 30, בעמ׳ 15-12.

[35] ראו: Simone Fischer-Hübner, *Privacy and Security at Risk in the Global Information Society*, in CYBERCRIME: LAW ENFORCEMENT SECURITY AND SURVEILLANCE IN THE INFORMATION AGE 173, 180 (D. THOMAS & B.D. LOADER, eds., 2000).

הגדרת תופעת ה"פצחנות" על מבצעיה איננה זוכה לפרשנות אחידה בחברה.[36] לצורכי מאמר זה טובה לי הגדרתו של פרופ' פורנל הרואה בפצחנות פעולה הכרוכה "בניסיון או חדירה לא מאושרת למערכות מחשב".[37] הגדרה זו תואמת את לשון חוק המחשבים, התנש"ה–1995, הקובע כי חדירה לחומר מחשב[38] שלא כדין היא עבירה, וכי יש לראות בכל "חדירה באמצעות התקשרות או התחברות עם מחשב, או על ידי הפעלתו" ככזו העונה על דרישות העבירה.[39] עוד קבוע בחוק כי אין הבחנה בין תוכנה

---

[36] לדיון נרחב בהגדרות השונות ראו: ENCYCLOPEDIA OF CYBERCRIME, HACKING AND HACKERS, 87 (SAMUEL C. MCQUADE III, ED., 2009).

[37] ראו: Steven Furnell, *Hackers, Viruses and Malicious Software*, *in* HANDBOOK OF INTERNET CRIME 173 (Y. JEWKES & M. YAR eds., 2010). קיימות גם הגדרות אחרות. כך לדוגמה בחוברת למהנדסי מחשבים מ-1975 הוצעה ההגדרה שלפיה פצחן הוא "אדם הנהנה לסייר בין פרטי מערכות ממוחשבות תוך ניסיון למתוח את גבולות היכולת שלהן, להבדיל ממשתמשים רגילים המעדיפים ללמוד רק את המינימום ההכרחי להפעלתן" (לדיון בהגדרה זו ובהגדרות אחרות ראו: Ben Yagoda, *A Short History of "Hack"*, THE NEW YORKER (Mar. 6, 2014) https://www.newyorker.com/tech/annals-of-technology/a-short-history-of-hack).
כתיבה אקדמית מודרנית עסוקה פחות בניסיון להגדיר את הפצחן ומתמקדת בסוגי פעולות פצחנות שונים. בבחירתי בהגדרה של פורנל אין אני מבקש לאמץ הגדרה אחת מחייבת אלא להתמקד בהגדרה שעוסקת רק בפעילות שנעדרת הסכמת המשתמש. בכך אני מבקש להבחין את הדיון ברשימה זו מדיונים אחרים בדבר פצחנות שכוללים גם פעולות פצחנות מצד פצחני הכובע הלבן או האפור.

[38] בפסיקה ניכרת פרשנות מרחיבה למונח מחשב (כך למשל בעניין **בדיר** נקבע כי המונח מחשב כולל גם מרכזיית טלפון ממוחשבת וגם מענה קולט ממוחשב, ראו: ת"פ (מחוזי ת"א) 40250/99 **מדינת ישראל נ' בדיר**, תק-מח 01(3) 1793 (2001); כפי שטוענת ד"ר גולדנברג-אהרוני, פרשנות זאת ראויה, שכן היא פותחת פתח ליישום החוק "לא רק על מחשבים קלאסיים", ובכך ניתן "מענה חקיקתי ראוי למגוון הפונקציות שממלא המחשב בחברה המודרנית". גולדברג-אהרוני חוזרת על עמדה זו במקום אחר שבו היא קובעת כי בתי המשפט נוטים לזהות קווי דמיון "בין מחשב לבין טלפון סלולרי, מבחינת הרציונל בבסיס הדין המיוחד למחשבים, מבחינת המידע המאוחסן בהם ודרך פעולתם". היא שבה וקובעת כי "גישה זו הנה ראויה, שכן יש להתרחק מהגישה שלפיה 'מחשב רגיל' הנו המחשב הביתי, עם צג ומקלדת" היא (וראו: שרון גולנדברג-אהרוני "חדירה למערכות מחשב - היקפה הרצוי והמצוי של העברה" **ספר דויד וינר** 429, 460–461 (2009) (לרבות שם בה"ש 115 ו-116).

[39] סעיף 4 לחוק המחשבים, התשנ"ה–1995; ד"ר גולדנברג-אהרוני מדגישה כי סעיף 4 לחוק המחשבים "פורש הגנה רחבה וראויה על המידע הממוחשב, שכן הוא חל על כל סוג של מידע ממוחשב (ולא על פלט), ללא קשר לאופיו ולחשיבותו" (שם, בעמ' 461).

למידע, ויש לראות בשניהם "חומר מחשב".[40] נשוב עוד להבחנות הקבועות בדין הישראלי בפרק ג.1. מטה.

לרשות הפצחן עומדים כלים שונים לטובת עצם ביצוע פעולת החדירה למחשב. הבולטת שבהם היא הנוזקה, תוכנה זדונית שנועדה לחדור למערכת מחשב ולבצע פעולות על המערכת, לרוב בהסתר. המונח "נוזקה" משמש שם כולל לשורה ארוכה של סוגי תוכנה שנועדו לחדור למערכות ולהפריע לפעולתן התקינה. עם אלה ניתן למנות וירוסים, תולעי מחשבים, סוסים טרויאנים, פצצות לוגיות, דלתות ממולכדות ותוכנות פרסום.[41] סוג מסוים של נוזקה הוא הרוגלה, שהיא המונחת בבסיס מאמר זה. במעבדות קספרסיקי מוגדרת הרוגלה "תוכנה שנועדה לאסוף מידע ממחשב או אמצעי אחר ולהעביר מידע זה לגורם שלישי ללא הסכמת או ידיעת המשתמש".[42] פעולות אלו כוללות לרוב איסוף מידע רגיש כדוגמת סיסמאות, מספרים אישיים מזהים (Personal Identification Numbers או PINs), ניטור של הקשת מקשים (Keyboard Sniffing), מעקב אחר פעילות גלישה באינטרנט וקצירה של כתובות דוא"ל, הפעלה של אפליקציות משנה (מצלמה, מיקרופון, מערכות איכון וכיו"ב).[43]

מבחינה זו צודקים בארגון Privacy International בטענתם כי לפעולות פצחנות יש פוטנציאל להיות פולשניות בהרבה מכל פעולת ריגול ומעקב אחרת מפני

---

[40] שם, סע' 1 (החוק מגדיר "מידע" כ"נתונים, סימנים, מושגים או הוראות, למעט תוכנה, המובעים בשפת קריאת מחשב". החוק ממשיך ומגדיר שפת קריאת מחשב כ"צורת הבעה המתאימה למסירה, לפירוש או לעיבוד על ידי מחשב או מחשב עזר בלבד" ותוכנה כ"קבוצת הוראות המובעות בשפה קריאת מחשב, המסוגל לקרום לתיפקוד של מחשב או לביצוע פעולה על ידי מחשב, והיא מגולמת, מוטבעת או מסומנת במכשיר או בחפץ, באמצעים אלקטרוניים, אלקטרומגנטיים, אלקטרוכימיים, אלקטרואופטיים, או באמצעים אחרים, או שהיא טבועה או אחודה עם המחשב באופן כלשהו או שהיא נפרדת ממנו").

[41] למידע נוסף על אמצעי תקיפה אלה ולדוגמאות לאופן השימוש בהם ראו: א' אינהורן ואח', **לוחמה בטרור בזירת המידע**, לעיל ה"ש 23, בעמ' 3–4.

[42] ראו: Kaspersky Lab, *What is Spyware? –Definition*, RESOURCE CENTER, https://usa.kaspersky.com/resource-center/threats/spyware.

[43] שם. ארגון הזכויות הדיגיטליות "גישה עכשיו" מונה פעילויות אפשרויות משימוש בתוכנות רוגלה על ידי גופי ביון ואכיפת חוק, ראו: AccessNow, *A Human Rights Response to Government Hacking*, 11–12 (Sep. 2016) https://www.accessnow.org/cms/assets/uploads/2016/09/GovernmentHackingDoc.pdf.

שחדירה לטכנולוגיות מרשתת הדברים (דוגמת סמארטפונים, מחשבים ניידים, חיישני רכב, טכנולוגיות בתים חכמים) מאפשרת איסוף מידע אינטימי ונרחב על המשתמש באופן שיאפשר חשיפה של זהותו, מחשבותיו, מערכות היחסים שלו, פעילויותיו ורצונותיו. יתרה מזאת, השימוש ברוגלה עלול להוות פתח לניצול הרסני בהרבה של חולשות המערכת שיאפשר השתלטות עליה ואז יהיה אפשר לא רק לנטר משתמשים ולעקוב אחריהם בזמן אמת (בשונה מאיסוף מידע פסיבי לאחר שנאגר) אלא גם להשפיע על אורחות חייהם.[44]

דמיינו בעיני רוחכם את ההבדלים בעבודתו של שוטר בחקירה פלילית של עבירת גידול סמים בין שנת 2000 לשנת 2017. בראשית המאה יכלו החוקרים לדרוש בצו את תצלומי הווידאו ממצלמת האבטחה של השכנים של החשוד. הם יכלו לבקש לקיים האזנת סתר באישור צו בית משפט על מכשיר הטלפון של החשוד וכן להתקין מכשיר איכון בתחתית רכבו של החשוד. הם יכלו לדרוש מידע שאגרה ספקית הסלולר של החשוד וכן לקדם מהלכים דומים נגד בני משפחתו ושותפיו. לעומת זאת ב-2017

---

[44] ראו: Privacy International's Analysis of the Italian Hacking Reform, under DDL Oralndo, 7 (Mar. 5, 2017), https://www.documentcloud.org/documents/3728074-Privacy-International-s-Analysis-of-the-Italian.html.
בדוח אחר שהגישו לוועדה לזכויות האדם של האו"ם הם טוענים כי תוכנות רוגלה הן למעשה "המרגל המושלם": "hacking grants authorities unrestricted and complete access and control over the device in question. The hacked device becomes the perfect spy, continuously and unabatedly sensing and monitoring the target's environment, to the whims of the controller. This includes, amongst other things: (1) the capturing of all incoming and outgoing data traffic (*e.g.* browsing history, email usage, content of communications, geospatial location, text messages, and photos); (2) the ability to switch on and off the microphone and camera of a device, without its owner's knowledge, (3) searching the hard drive and making copies of all or part of the computer system's memory units; (4) deciphering everything that is typed on the keyboard, using key-loggers, and collecting anything that is seen on the screen, by taking screenshots, regardless of whether the owner had used encryption software". ראו: Joint Submission, *Privacy International and the Italian Coalition for Civil Liberties, Consideration of the Sixth Periodic Report of Itality*, Human Rights Committee 119th Session, 2 (Feb. 6, 2017), https://tbinternet.ohchr.org/Treaties/CCPR/Shared%20Documents/ITA/INT_CCPR_CSS_ITA_26517_E.pdf.

כל שהם יזדקקו לו היא פעולת פצחנות מוצלחת אחת, למכשיר הנייד של החשוד, ואיסוף הן בזמן אמת והן בזמן מנוחה של כל המידע שהמכשיר נגיש אליו אשר יכלול מן הסתם את כל סוגי המידע שאוזכרו לעיל. יתרה מזאת, השתלטות על רכבו של החשוד, על מערכת החשמל בביתו או על קוצב הלב שלו עשויים להעניק לאותו השוטר כוח חסר תקדים במעקב אחר חשודים.

מנגד חשוב להכיר גם בצורך בפיתוח כלים טכנולוגיים לעבודת גופי האכיפה. השימוש ההולך וגובר בשרתי "ניתוב בצל" (The Onion Routing או TOR), קרי השמשתה של רשת פרטיות בקוד פתוח המאפשרת למשתמשים לגלוש אנונימית באינטרנט, הולידה עימה ברבות השנים את תופעת "הרשת האפלה" (Dark Web) כשטח שחסין בפני מרבית שיטות הריגול והמעקב.[45] הגם שכלי אנונימיזציה רשתיים מספקים שירות חשוב בהגנת חופש הביטוי, הפרטיות וההתאספות בחברה דמוקרטית,[46] השימוש בהם למטרות פשיעה הופך את יכולתם של גופי אכיפת החוק

---

[45] לקריאה נוספת על הרשת האפלה ראו: עודד ירון "הצדדים המוארים של הרשת האפילה יכולים להציל את כולנו" **הארץ** (19.2.2017) https://www.haaretz.co.il/captain/net/.premium-MAGAZINE-1.3871060. כפי שמתאר ירון, הרשת האפלה נשענת על נתב הבצל בניסיון להעביר את כל המידע הזורם ברשת האנונימית "דרך כמה צמתים, ובכל שלב להוסיף לו שכבת הצפנה". בכך למעשה מתאפשרת רשת תקשורת נפרדת לאינטרנט שבה מתנגדי משטר דכאני ופעילי זכויות אדם יכולים לשוחח ולהתאגד, אך כמוהם גם אלו המבקשים להשתמש ברשת למטרות הימורים לא חוקיים, סחר בסמים ובבני אדם, וכן צריכה של פורנוגרפיית ילדים. עם זאת כפי שמדגיש ירון על פי הערכות זהירות רק כ-20%–30% מהרשת האפלה משמשים למטרות פליליות או זדוניות.

[46] ראו דבריו של הדווח המנחה לחופש הביטוי של המועצה לזכויות האדם של האו"ם, Human Right Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, U.N. Doc. A/HRC/29/32, paras. 9, 12-13 (May. 22, 2015). ("Anonymity is the condition of avoiding identification. A common human desire to protect one's identity from the crowd, anonymity may liberate a user to explore and impart ideas and opinions more than she would using her actual identity... encryption and anonymity, separately or together, create a zone of privacy to protect opinion and belief... Journalists, researchers, lawyers and civil society rely on encryption and anonymity to shield themselves (and their sources, clients, and partners) from surveillance and harassment. The ability to search the web, develop ideas and communicate securely may be the only way in which many can explore basic aspects of identity, such as one's gender, religion, ethnicity, national origin, or secxuality... The "dark" side of

להשלים את משימתם לקשה בהרבה.[47] פיתוח כלים ומתודות התמודדות עם הגידול בתופעת עבירות סייבר ברשת האפלה, על שלל מרכיביה, הוא צורך חיוני של המדינה המודרנית ומעוגן בזכותה, שהיא גם חובתה, להגן על גבולותיה ועל אזרחיה מפני פשיעה חוצת-גבולות ואיומים על ביטחון המדינה.

לשם הבנה מלאה של השדה הטכנולוגי נכון להתעכב על מרכיביה השונים של הנוזקה, לרבות נוזקות מסוג רוגלה. בהקשר זה אני מבקש להשתמש במודל PrEP שתבע טריי הר, עמית סייבר באוניברסיטת הרווארד (ראו המחשה ויזואלית של המודל בנספח 1 למאמר זה). על פי המודל של הר, כל נוזקה מורכבת משלושה מרכיבים שונים: (1) מתודת ההתפשטות (Propagation Method); (2) הקוד המנצל (Exploit); (3) המטע"ד (Payload).[48] נעמוד על כל אחד ממרכיבים אלה.

2.א. מתודת ההתפשטות (Propagation Method)

מתודת ההתפשטות היא השיטה שבה מועבר הקוד הזדוני מהמקור אל היעד. ייתכנו כמה שלבים בתהליך ההתפשטות, וייתכן שהוא יכלול כמה מתודות התפשטות שונות לאורך התהליך. מתודות ההתפשטות מובחנות אלה מאלה ברמת הדיוק שלהן

---

encryption and anonymity is a reflection of the fact that wrongdoing offline takes place online as well"). עוד ראו שם ("יש בהחלט תוכן רע בדארקווב. אין דרך לייפות את זה", סיפרה ל"הארץ" שרה ג'יימי לואיס, חוקרת עצמאית של פרטיות, אנונימיות והדארק ווב. "מדובר בכלים נגד צנזורה והם משמשים הרבה אנשים, כולל כאלה שרוצים לבצע פעילויות בלתי חוקיות. אבל, כשאתה מסתכל על הדארקווב, ועל התוכן שקיים בה, אפילו המחקרים המוטים ביותר לא מגיעים ליותר מ-50% תוכן בלתי חוקי").

[47] ראו: Letter from Mythili Raman, Acting Assistant Attorney Gen., Criminal Div., U.S. Dep't of Justice, to Judge Reena Raggi, Chair, Advisory Comm. on Rules of Criminal Procedure 4 (September 18, 2013), in Advisory Committee On Rules of Criminal Procedure: April 2014, 2 (2014), https://www.uscourts.gov/sites/default/files/fr_import/CR2014-04.pdf (שם מציינת סגנית התובע הכללי כי "There is a substantial public interest in catching and prosecuting criminals who use anonymizing technologies, but locating them can be impossible for law enforcement absent the ability to conduct a remote search of the criminal's computer").

[48] ראו: Trey Herr, *PrEP: A Framework for Malware & Cyber Weapons*, 13(1) J. INFO. WARFARE 87 (2014).

ובמגבלות הטכניות שלהן, ולכן היקף הפגיעה שלהן יכול שיהיה מצומצם יותר או רחב יותר. כך לדוגמה אין דין תולעת דוא"ל כדין אתר אינטרנט עם קישור זדוני, ואין דין אלה כדין כונן חיצוני "מטופל" שעליו מותקנת התוכנה הזדונית.[49]

שתי מתודות התפשטות ראויות להתייחסות מיוחדת: הראשונה היא מתודת "ההנדסה החברתית" (Social Engineering), והיא כוללת התאמה אישית של מתודת ההתפשטות למאפיינים של המטרה. הרשות הלאומית להגנת הסייבר מגדירה את המתודה: "ניצול תכונות פסיכולוגיות אנושיות, לטובת הונאה, שכנוע והתחזות, המביאות את האדם לציית מרצון לבקשת התוקף ולמסור לידיו מידע אישי אודותיו או אודות ארגונו".[50] אם בראשית ימי האינטרנט היינו עדים לתופעה של דִּיוּג (Phishing) כללי, קרי ניסיון לגנבת מידע באמצעות דואר זבל אלקטרוני (מוכרת במיוחד הונאת "העוקץ הניגרי"),[51] כיום מקובל דווקא לעסוק בדיוג באמצעות חנית

---

[49] שם, בעמ' 88–89 טריי מונה שורה של דוגמאות למתודות התפשטות שונות, ובהן Compromised Computer, Compromised Certificate Authorities, Compromised email attachment or URL, Dropper Software, Local Area Network, Removable Storage Media.

[50] ראו: "מהי הנדסה חברתית" **הרשות הלאומית להגנת הסייבר** (26.5.2015) https://www.gov.il/he/Departments/publications/reports/social_engineering (הרשות ממשיכה להסביר כי: "הנדסה חברתית אינה מוגבלת למפגש פנים אל פנים. היא יכולה להתבצע באמצעות טכנולוגיות מגוונות: לדוגמה, בשיחת טלפון, בדואר אלקטרוני, סמס, פנייה בפייסבוק, טוויטר, צ'אט או שיחה מקוונת. לעיתים התוקף אף יכול לשלב מהלך כפול, ראשית ישלח לקורבן דואר אלקטרוני ולאחריו ישלח הודעת סמס שתעצים בקורבן את תחושת האמינות. דוגמה נוספת היא בעת ביקור בשירות בנקאי מקוון ישלח התוקף דואר אלקטרוני המתחזה לשירות הבנקאי המבקש את עדכון הפרטים האישיים... תוקף הממוקד במטרתו לא ישקוט. במידה ולא הצליח לאסוף מספיק מידע מהמקור הראשון, ישתמש בפיסות המידע שאסף להגברת אמינותו, ויפנה למקור אחר בארגון וכך הלאה עד להשגת מבוקשו").

[51] לרוב בצורת פנייה מצד אזרח ניגרי המבקש להעביר מיליוני דולרים לחשבונות בנק בארצות הברית ומבטיח לשלם סכומים נכבדים לגורם שיסכים לסייע. הונאות מסוג אלה מזכירות את "הונאת האסיר הספרדי" אשר תועדה לראשונה במאה השש-עשרה שבה קורבנות ההונאה קיבלו מכתב ממישהו אנונימי שטען כי נעצר על לא עוול בכפו במהלך ביקור בספרד ומבקש סיוע כלכלי כדי לקנות בחזרה את חפותו. בתמורה הוא מתחייב כי ישלם בעין יפה לכל מי שיסייע לו עם צאתו מהכלא. לקריאה נוספת ראו: גיל נוילנדר, "הונאת "העוקץ הניגרי" משפרת את העברית", **News1** 21.10.2014 https://www.news1.co.il/Archive/0024-D-96794-00.html.

(Spear Phishing) שהיא דיג ממוקד יותר.[52] הרעיון הוא לא לזרוק חכה למים ולחכות לקורבן אקראי, אלא לבחור בעצמנו מראש את הקורבן ולהשליך לכיוונו חנית כדי לתפוס אותו ספציפית. אלה הן מתקפות של הנדסה חברתית, המחייבות את התוקף לפתח אינטימיות עם המטרה ולזהות את מאפייני הפעילות שלו או שלה ברשת. הגם ששיטות אלה כרוכות בעלות גבוהה יותר מבחינת זמן וכוח אדם, סיכויי ההצלחה שלה גוברים. פרשת הריגול המקסיקנית שתוארה לעיל היא דוגמה טובה של מתקפת "הנדסה חברתית". הודעות הטקסט הפותחות את הכתבה נכתבו במיוחד ליעדים הספציפיים שהותקפו. לעומת זאת מתקפת Wannacry הייתה הרבה פחות ממוקדת או מתוחכמת וכללה מתקפת דיוג בסיסית בתחילה ולאחר מכן התפשטות על דרך של תולעי דוא"ל ברחבי הרשת הפנימית.

מתודת התפשטות נוספת היא "מתקפת באר המים", והיא כרוכה בניצול אתרים לא מאובטחים שאליהם המטרות נוהגות לגלוש. בחלק מהמקרים המתקפה תחייב את הגולש להקיש על מודעה גרפית (באנר) או קישור ספציפיים או להוריד דבוקה ספציפית (מה שמכונה "הורדת רכב חולף" או Drive By Download). כל מי שיוריד את הדבוקה למחשבו, כאילו שתה מהבאר המורעלת, ובכך יאפשר את גישת הנוזקה אל מחשבו. כך לדוגמה ביוני 2017 התקבלו ידיעות על מתקפת כופר נרחבת שהחלה באוקראינה והתפשטה למדינות נוספות בכל רחבי העולם, ובעיקר באירופה.[53]

---

[52] "דייג אוהב דגים? – על התקפות Spear Phising" **האקר את האוייב** 26.5.2012 (אם במתקפת פישינג, https://samorai88.wordpress.com/2012/05/26/spear-phishing/ התוקף מסתמך על שליחת הפיתיון למספר רב של אנשים מתוך ידיעת הסבירות הסטטיסטית שקיים שיעור כלשהו שיתפתה "לנשוך בחכה", הרי שמתקפת Spear-Phising היא מתקפה מממוקדת, בדומה לדייג המחזיק חנית ומנסה לנעוץ אותה בנקודת זמן מסוימת ובדג ספציפי. מתקפות Spear-Phising הן הונאות המבוצעות לרוב באמצעות דוא"ל (אך לא בהכרח), ואשר שמות להן למטרה ארגון ספציפי, בחיפוש אחר מידע רגיש. העומדים מאחורי מתקפות מסוג זה אינם על פי רוב "האקרים אקראיים" כי אם תוקפים מיומנים שמטרתם להשיג רווח כלכלי, סודות תעשייתיים או מידע צבאי/מדיני. הודעות פישינג "רגילות" תמיד ינסו להיראות כאילו הן מגיעות ממקור אמין, לרוב חברה גדולה ומוכרת, כגון בנק הפועלים, Paypal, eBay וכיו"ב. במקרה של Spear-Phising, המקור של המכתב אף עלול להיראות כאילו נשלח בידי אדם ספציפי מתוך הארגון של הנמען, לרוב מישהו בעמדת כוח).

[53] לקריאה נוספת ראו: *Spear-Phising, Watering Hole and Drive-by Attacks: The New Normal White Paper*, INVINCEA (May. 2013) https://www.slideshare.net/Invincea/invincea-spearphishingwateringholedrivebywhitepaper51713.

אחת ממתודות ההתפשטות של אותה מתקפה כללה "מתקפת באר מים" דרך אתר חדשות אוקראיני מקומי ואתר האינטרנט של עיריית בחמוט. בשני המקרים כללו הפצחנים תקיפות "הורדת רכב חולף".[54]

2.ב. הקוד המנצל (Exploit)

הקוד המנצל, מסביר הר, נכתב כדי לנצל טעויות תוכנה ובכך לפתוח את הדלת לאופרציה של יתר מרכיבי הנוזקה, בין שזו מתודת ההתפשטות או המטען הייעודי (מטע"ד).<בסדר?> הקוד המנצל מובחן מהמטע"ד, שכן מטרתו אינה ליצור אפקט כלשהו על המערכת (מה שהר מכנה writing to the effect), אלא להתאים את הנוזקה למאפיינים הספציפיים של החולשה שאותה היא מבקשת לנצל (מה שהר מכנה writing to the target). עוד מבחין הר בין שלוש קטגוריות שונות של קודים מנצלים: אלה שנועדו לאפשר את הגישה למערכת המותקפת (ולרוב יסייעו למימוש מתודת ההתפשטות) ואלה שנועדו לעודד הסלמה בהיקף זכויות היתר הניתנות לנוזקה (Escalation of Privileges) או לאפשר את ההוצאה לפועל של הנוזקה (Code Execution) (ולרוב יסייעו למימוש המטע"ד). כפי שכבר צוין לעיל, אנו נוטים לסווג קודים מנצלים שונים לפי זמן החשיפה של היצרן לקיומה של החולשה (ראו הדיון לעיל בדבר חולשות אפס-ימים).[55] כפי שראינו בפרשת Wannacry, הסוכנות לביטחון לאומי בארצות הברית זיהתה פרצת אבטחה במערכת ההפעלה windows וכתבה עבורה קוד מנצל לטובת עבודתה השוטפת כארגון ביון. אלא שהקוד והכלים של

---

[54] ראו: "עדכון: מתקפת כופר נרחבת ברחבי העולם נכון ל-20:14" **הרשות הלאומית להגנת הסייבר** 29.6.2017 www.gov.il/he/Departments/publications/reports/petya_report.
עוד ראו: Tom Spring, *Researchers Find Blackenergy Apt Links in Expetr Code*, THREAT POST (Jul. 3, 2017) https://threatpost.com/researchers-find-blackenergy-apt-links-in-expetr-code/126662/.

[55] ראו: טריי הר, לעיל ה"ש 48, בעמ' 91–92.

הסוכנות נגנבו בידי "מתווכי הצללים", פורסמו ברבים והושמשו בהמשך בידי התוקפים.[56]

2.ג. המטע"ד (Payload)

המטע"ד הוא התוכן המרכזי של הנוזקה. קוד זדוני שנועד להוציא אל הפועל על המחשב או המערכת המותקפת פעולות שהתקף קבען מראש. המטע"ד יכול שיהיה פשוט או מתוחכם, יכול שיכלול פעולה אחת או פעולות אחדות ויכול לשרת מטרה אחת או מספר רב של מטרות. אנו נוטים לסווג את הנוזקה על פי המטע"ד שבחיקה. כך מטע"ד שמתמקד באיסוף מידע מהמערכת המותקפת (מטע"ד ריגול) יקים נוזקה מסוג רוגלה (וראו לדוגמה מערכת "פגסוס" של חברת NSO הישראלית). לעומת זאת מטע"ד שמתמקד בהצפנת מידע ושחרורו בתשלום (מטע"ד דיסאינפורמציה) יקים נוזקה מסוג כופרה (כמו במקרה של פרשת Wannacry). הר מבחין בין שישה סוגים של מטע"דים: (1) **ריגול** – מטע"ד שנועד לגנוב מידע מהמשתמש או מהמערכת; (2) **ניצול משאבים** – מטע"ד שנועד לצרוך משאבי מערכת לדוגמה בהקשר של התקפת מניעת שירות מבוזרת או DDoS);[57] (3) **דיסאינפורמציה** – מטע"ד שנועד לשנות מידע על המערכת ללא ידיעת המשתמש; (4) **איפול** – מטע"ד שנועד להסתיר את הנוזקה מפני זיהוי באמצעות מערכות ההגנה שעל המערכת; (5) **שליטה ובקרה** – מטע"ד שנועד לתקשר החוצה מהמערכת המותקפת, ובמקרים מסוימים לקבל מודולי המשך

---

[56] איתן בייגל "מתקפת הסייבר הגדולה – מה בדיוק קרה, ואיך זה התבצע?" **גלובס** 14.5.2017 https://www.globes.co.il/news/article.aspx?did=1001188447.

[57] התקפות מניעת שירות נועדו להשבית מערכת מחשב באמצעות יצירת עומס חריג על משאביה. בהעמסת משאבי מחשב מסוימים נמנעת גישתם של המשתמשים לאותו המשאב. בהתקפת מניעת שירות מבוזרת מבוצעת ההתקפה באמצעות כמה מחשבים מסונכרנים, ובחלק מהמקרים באמצעות "צבא זומבים" (כמה מחשבים שהשתלטו עליהם והם מנוצלים מרחוק למטרות התקיפה, לעיתים מכונים גם "מערכי רובורשת", וראו הרחבה בגוף המאמר). להרחבה ראו: "התקפות מניעת שירות (DOS), התמודדות החוק הפלילי, המשטרה, ובתי המשפט בישראל", **גיא אופיר משרד עורכי דין** http://www.ophirlaw.com/%D7%94%D7%AA%D7%A7%D7%A4%D7%AA-dos/.

למטע"ד לביצוע תקיפות נוספות; (6) **התמדה** – מטע"ד המבטיח המשך גישה למערכת גם לאחר זיהוי והסרה של הנוזקה הראשונית.[58]

תופעת "מרשתת הדברים" מעודדת כניסתן של טכנולוגיות מקושרות אשר על פי רוב מוגבלות ברמת הגנת הסייבר המובנית בהן לתוך הבתים ולשימושם האישי של מיליוני צרכנים. הגידול המהיר בתופעה מעודד פצחנים לפתח מטע"דים שעיקר ייעודם לייצר מערכי רובורשת (או Botnet). הרובורשת הוא מערך של מחשבים המקושרים לשרת שליטה מרכזי, ובשעת קריאה ערוכים לממש "משימה זדונית" עבור מי ששולט בהם בנצלם את המשאבים של המחשבים ברשת כולה (ראו בהקשר זה נספח 2 למאמר זה, הכולל המחשה של משרד מבקר המדינה להתגלגלות מערך רובורשת).

ג. מיפוי השדה המשפטי

בהישען על הידע הטכנולוגי שתואר לעיל, רשימה זו ממשיכה לסקור את עיקרי המסגרת המשפטית המסדירה פעולות פצחנות למטרות מאבק בטרור בדין הישראלי, הבין-לאומי והמשווה. פרק זה מבקש לדון במגבלות הדין הקיים בישראל ובתמצית הצעת החוק התלויה ועומדת בפני ועדת החוקה, חוק ומשפט של הכנסת. פרק זה מבקש עוד להציג את המסגרות המשפטיות הקיימות בדין הזר, הבין-לאומי והמשווה, מתוך תקווה כי אלה יסייעו בידינו בגיבוש המלצות מדיניות למחוקק, אשר יידונו בהרחבה בפרק ד.

1. הדין הישראלי

1.א. הדין הקיים

מן המקובל כי בפתח דיון בשאלות של פעילות מעקב והאזנה בדין הישראלי יציין המתדיין את המובן מאליו. הזכות לפרטיות עוגנה בסעיף 7 לחוק-יסוד: כבוד

[58] ראו: טריי הר, לעיל ה"ש 48, בעמ' 92–93.

האדם וחירותו ומוכרת כזכות חוקתית שכל פגיעה בה תיעשה אך ורק לפי התנאים שנקבעו בפסקת ההגבלה שבסעיף 8 לחוק היסוד.[59] לא זאת בלבד, הכנסת חוקקה גם את חוק הגנת הפרטיות, שקובע כי פגיעה בזכות (לדוגמה על דרך של מעקב אחרי אדם, האזנה אסורה על פי דין או צילום אדם ברשות היחיד) היא עבירה פלילית ועוולה אזרחית.[60] זאת ועוד, הזכות החוקתית לפרטיות, כאחת "מזכויות-העל",[61] עשויה להקרין על פרשנותם של דברי חקיקה אחרים, ובראשם חוק הגנת הפרטיות שקדם לחקיקת חוק היסוד. לא מפתיע אפוא כי יש בכותבים מי שכבר הצביעו על "המהפכה החוקתית של הזכות לפרטיות" בדין הישראלי בקובעם כי "ההפרה של הכללים החלים על הגנת מידע אישי במאגרי מידע אינה נתפסת כהפרה טכנית, נומינלית, אלא כפגיעה בזכות יסוד חוקתית. בכך מתקרבת ישראל לתפיסה האירופית שלפיה הזכות לפרטיות כוללת גם זכות ל-Informational Self Determination, קרי: זכות לשליטה על מידע אישי במאגרי מידע".[62]

---

[59] סעיפים 7–8 לחוק-יסוד: כבוד האדם וחירותו; לשעבר הנשיא ברק התייחס לשאלת היקפה של הזכות בקובעו כי "הזכות החוקתית לפרטיות משתרעת בין השאר – ובלא כל ניסיון להקיף את הזכות על כל היבטיה – על זכותו של אדם לנהל את אורח החיים בו הוא חפץ בד' אמות ביתו, בלא הפרעה מבחוץ. ביתו של אדם הוא מבצרו, ובגדריו הוא זכאי לכך כי יניחו אותו לעצמו, לפיתוח האוטונומיה של הרצון הפרטי שלו". ראו: בג"ץ 2481/93 **יוסף דיין נ' ניצב יהודה וילק**, פ"ד מח(2) 456, 469 (1994); ראו עוד בג"ץ 6650/04 **פלוני נ' בית הדין הרבני האיזורי בנתניה**, פ"ד סא(1) 581, בסעיף 8 לפסק דינו של הנשיא ברק (2006); השופטת דורנר קבעה עוד כי "הוראות סעיף 11 לחוק היסוד, המטילה על רשויות המדינה את החובה לכבד את הזכויות המעוגנת בו, אף מחייבת את בית המשפט לתת פירוש דווקני לחוקים הפוגעים בפרטיות, לרבות לחוקים שתוקפם נשמר מכוח סעיף 10 לחוק היסוד". ראו: בש"פ 537/95 **גנימאת נ' מדינת ישראל**, פ"ד מט(3) 355, 375(1995); לאחרונה הביעו שופטי בית המשפט העליון עמדה ערכית באשר להיקף תחולת הזכות לפרטיות על טכנולוגיות מודרניות, דוגמת טלפונים חכמים. הנשיאה נאור ציינה בדיון כי "טלפון זה להיכנס עמוק לנשמה, הרבה יותר מאשר להיכנס לבית". ראו: אשר הלפרין "נאור על חיפוש בטלפון של נחקר: 'כמו להיכנס עמוק לנשמה'" **וואלה! חדשות** 19.6.2017 https://news.walla.co.il/item/3074512.

[60] סעיפים 4–5 לחוק הגנת הפרטיות, התשמ"א–1981.

[61] ע"א 8825/03 **שירותי בריאות כללית נ' משרד הבטחון**, פס' כ"א לפסק דינו של השופט רובינשטיין (פורסם בנבו 11.4.2007).

[62] עומר טנא "הזכות לפרטיות בעקבות חוק יסוד כבוד האדם: מהפך מושגי, חוקתי ורגולטורי" **קרית המשפט** ח 39, 68–69 (2009). דוגמה אחת להקרנה של חוק היסוד על חוק הגנת הפרטיות יכול שתימצא במעבר של בתי המשפט ממבחנים פרשניים הנשענים על מסגרת האיזונים הקבועה בחוק הגנת הפרטיות למבחנים פרשניים הנשענים דווקא על מערכת האיזונים הקבועה בסעיף 8 לחוק היסוד. כך היה למשל בפרשת **שאלתיאל נ' בנק המזרחי**,

הזכות לפרטיות היא "מהחשובה שבזכויות האדם... היא 'אחת החירויות המעצבות את אופיו של המשטר בישראל כמשטר דמוקרטי והיא אחת מזכויות העל המבססות את הכבוד והחירות להן זכאי אדם כאדם, כערך בפני עצמו'".[63] זכות חוקתית על-חוקית היא "מותחת קו בין הפרט לבין הכלל, בין ה'אני' לבין החברה. היא משרטטת מיתחם אשר בו מניחים את הפרט לנפשו, לפיתוח 'האני' שלו, בלא מעורבות של הזולת".[64] הזכות מקימה למתדיינים הישראלים מגן ממשי מפני חדירה לא רצויה, וודאי שלא מוסכמת, למרחבי הפרט – בין שבוצעה בידי יחיד ובין שבוצעה על ידי תאגיד או רשות מרשויות המדינה.

עם זאת הזכות לפרטיות אינה מוחלטת, וניתן לפגוע בה, בין היתר לשם מניעת עבירות ולהגנה על ביטחון המדינה.[65] כך לדוגמה סעיף 19 לחוק הגנת הפרטיות מחריג את רשויות הביטחון – המשטרה, אגף המודיעין בצה"ל, המשטרה הצבאית, השב"כ, המוסד והרשות להגנת עדים – מתחולת החוק בתנאי שפגיעתם בפרטיות "נעשתה באופן סביר במסגרת תפקידם ולשם מילויו".[66]

המסלול הטבעי לפעילויות מעקב והאזנה מצוי בחוק האזנת סתר.[67] החוק מבחין בין האזנת סתר שמטרתה ביטחון המדינה (פרק ב) להאזנת סתר שמטרתה

שעניינה חשיפת מידע פיננסי של לקוחה על ידי בנק למעסיקיה, ללא ידיעתה או הסכמתה. בית המשפט מציין בעניין זה כי "העלאת הזכות לפרטיות למעלת זכות יסוד מוגנת, מטה את הכף עוד יותר לכיוון חיזוק הסודיות הבנקאית והגנה על המידע הקשור בלקוח. כאמור, סעיף 20 לחוק הגנת הפרטיות, קובע כי ההגנה של עניין אישי כשר תעמוד רק אם, הפגיעה לא חרגה מתחום הסביר באותן נסיבות'. אם נתרגם דרישת הסבירות לשיח החוקתי דהיום, נשתמש במבחן המידתיות שהוא מבחן משכולל ומפותח יותר ממבחן הסבירות" (ת"א (עכו) 2483/97 **שאלתיאל נ' בנק המזרחי המאוחד בע"מ**, תק-שלום 99(3), 2625 (1999)).

[63] עניין **שירותי בריאות כללית**, לעיל ה"ש 61, שם.

[64] ראו: עניין **דיין**, לעיל ה"ש 59, בעמ' 471.

[65] ראו: ב"ש (ת"א) 90868/00 **חברת נטוויז'ן בע"מ נ' צבא הגנה לישראל** (פורסם בנבו 22.6.2000) ("ריסון הרשויות מפני פגיעה בפרטיות השיח בעידן של תקשורת מודרנית אינו תמיד אפשרי, גם אם רצוי, כאשר מנגד עלול להיפגע אינטרס חיוני אחר של הציבור").

[66] סעיף 19 לחוק הגנת הפרטיות; ד"ר אהרוני-גולדנברג מבקרת פטור זה וקובעת כי הוא גורף מדי. ראו: גולדנברג-אהרוני, לעיל ה"ש 38, בעמ' 478, ה"ש 193.

[67] משה שלגי וצבי כהן מנו בספרם שורת שיקולים שעל השופט לבחון בטרם יאשר בקשה למתן היתר להאזנת סתר: (1) חשד לביצוע עבירה חמורה שיש לציבור עניין ממשי במניעתה או בגילוי מבצעי, אשר גובר על עניין הציבור בהגנה על פרטיותם של האנשים שהבקשה נוגעת אליהם; (2) ההאזנה נחוצה ואין שיטות חקירה אחרות שעשויות להבטיח בסבירות את מטרות החקירה; (3) אם מתקיים חשד כלפי הנוגעים בדבר במידה המספקת להצדקת הפגיעה בפרטיותם על דרך של האזנת סתר; (4) המספר המשוער של אנשים אשר עשויים להשתמש

מניעת עבירות וגילוי עבריינים (פרק ג) וקובע בהתאמה שני מסלולים: מסלול נוקשה ומסלול מקל, לפי סוג ההאזנה המתבקשת. ד"ר פוקס מציע סיכום של עיקרי מסלולים אלה:

> "כאשר ההאזנה נעשית לצורכי אכיפת חוק רגילה, היא חייבת להיות מאושרת על ידי נשיא בית משפט מחוזי או סגנו. צו כזה יינתן רק אם השופט שוכנע, 'לאחר ששקל את מידת הפגיעה בפרטיות', שהדבר דרוש לצורכי חקירה או למניעת עברות מסוג פשע. הצו חייב לציין אם הפרטים ידועים, את שם האדם לו מותר להאזין או את זהות הקו לו מאזינים ואת מקום השיחות. כן יפורטו בצו דרכי ההאזנה. כל צו יינתן לתקופה של עד שלושה חודשים, הניתנת להארכה. בכל חודש על מפכ"ל המשטרה לדווח ליועץ המשפטי לממשלה על מספר ההיתרים שניתנו ופעם בשנה על השר לביטחון פנים לדווח לוועדת החוקה, חוק משפט של הכנסת על מספר הבקשות שהוגשו ומספר ההיתרים שניתנו, כולל מספר האנשים ומספר הקווים שלהם התירו האזנה. במקרים דחופים, כאשר מפכ"ל המשטרה משוכנע שלא ניתן לדחות את ההאזנה עד לקבלת צו משופט, הוא רשאי להתיר האזנת סתר לתקופה שלא תעלה על 48 שעות. היועץ המשפטי לממשלה רשאי לבטל היתר זה ושופט בית משפט מחוזי יכול לאשר אותו בדיעבד.
>
> האזנה מטעמים של ביטחון המדינה נעשית על סמך אישור של ראש הממשלה או שר הביטחון לבקשת ראש השב"כ או ראש המודיעין הצבאי, ללא צורך בהליך שיפוטי. גם בהיתר זה צריך לציין את זהות האדם לו הותרה ההאזנה או את זהות הקו ואת מקום השיחות. כן יש לפרט את דרכי ההאזנה. אישור כזה ניתן אף הוא לתקופה של עד שלושה חודשים, הניתנת להארכה. אחת לשלושה חודשים על שר הביטחון לדווח ליועץ המשפטי לממשלה על היתרים שניתנו לפי החוק, ופעם בשנה יימסר דיווח על מספר ההיתרים שניתנו לוועדה משותפת של ועדת חוקה, חוק ומשפט

בטלפון המואזן (בשל החשש מפני איסוף של מידע אגבי); (5) זהות האנשים אשר פרטיותם עלולה להיפגע, מיקומם וזכאותם להגנות נוספות על פי דין; (6) אם התקופה המבוקשת חיונית. ראו: משה שלגי וצבי כהן **סדרי הדין הפלילי** 71–77 (מהדורה שניה, התשס"א).

> וועדת חוץ וביטחון היושבת בדלתיים סגורות. במקרים דחופים יכולים ראש השב״כ או ראש אגף המודיעין של צה״ל להתיר האזנה כזו לתקופה של עד 48 שעות והיועץ המשפטי לממשלה, שר הביטחון או ראש הממשלה רשאים לבטל היתר זה״.[68]

גדי אשד, לשעבר מפקד ימ״ר תל אביב, מונה שישה סטנדרטים שנקבעו בפסיקה בדבר הקבילות הטכנית של הקלטות כחלק מהכשרתן כראיות: תקינות המכשיר המקליט, מיומנות המפעיל, מהימנות ההקלטה, עמידה בעקרון ההגנה על השרשרת הראייתית (קרי לא בוצעו בהקלטה שינויים, תוספות או השמטות), זיהוי הקולות בהקלטה וכן כי ההקלטה מבטאת רצון חופשי של הדובר.[69] סעיף 13 לחוק האזנות סתר עיגן כלל פסילה ראייתי הדומה במהותו לדוקטרינת ״הפרי המורעל״ האמריקאית, בהתאמות מסוימות, ולפיו אי-עמידה בהוראות החוק פירושה כי הראיות לא יהיו קבילות בבית משפט.[70] אשד מתאר את הסעיף כ״אקט 'מחנך' ... שרואה בפסילה מעין תמרור אזהרה כנגד רשויות האכיפה, ובמקביל מגן על זכויותיו של האזרח״.[71]

נסיט כעת מבטנו לעבר חומר מחשב. מאמר זה אין עניינו בתפיסה פיזית של מחשבים וטלפונים חכמים על ידי גופי אכיפה אגב חיפוש בבית או במוסד.[72] כמו כן

---

[68] עמיר פוקס ״מגבלות משפטיות על איסוף מודיעין – המשפט הישראלי״ **פרטיות בעידן של שינוי** 259, 262–263 (תהילה שוורץ-אלטשולר עורכת, 2012). להרחבה ראו גם: עמיר כהנא ויובל שני, **רגולציה של מעקב מקוון בדין הישראלי ובדין המשווה** 42–52 (2019).

[69] גדי אשד ״'אוזניים לכותל': האזנות סתר בעידן החדש״ **משפט וצבא** 16 (התשס״ג) 585, 607–608.

[70] סעיף 13 לחוק האזנת סתר, התשל״ט–1979. חריג לכלל פסלות הראיות הוא הקלטה שאומנם התקבלה כחלק מהאזנה אסורה אך הוקלטה בהליך פלילי של פשע חמור (שעונשו מאסר של יותר משבע שנים). זאת, רק באישור בית המשפט מטעמים מיוחדים ולאחר שנשתכנע השופט כי ״הצורך להגיע לחקר האמת גובר על שיקולי הפרטיות״. ראו: כהנא ושני, לעיל ה״ש 68, בעמ׳ 51.

[71] אשד, לעיל ה״ש 69, בעמ׳ 609.

[72] חיפוש שכזה כפוף לפקודת סדר הדין הפלילי (מעצר וחיפוש) [נוסח חדש], התשכ״ט–1969, הקובע בסעיף 32(א) כי ״רשאי שוטר לתפוס חפץ, אם יש לו יסוד סביר להניח כי באותו חפץ נעברה, או עומדים לעבור, עבירה, או שהוא עשוי לשמש ראיה בהליך משפטי בשל עבירה או שניתן כשכר בעד ביצוע עבירה או כאמצעי לביצועה״. סעיף 32(ב) מחריג בהקשר זה תפיסת מחשב או דבר המגלם חומר מחשב אם הוא בשימוש של מוסד (דוגמת בית עסק). במקרים אלו נדרש צו מפרש של בית משפט השלום. החוק קובע עוד כי אם הציוד אינו דרוש עוד לצורך הגשתו כראיה לבית המשפט, על המשטרה להחזירו לאדם שממנו נלקח בתוך 30 ימים מיום

מוחרג מגבולות מאמר זה הדיון, המרתק כשלעצמו, בשאלת הסמכות לדרוש מצדדים שלישיים (דוגמת ספקי שירותי אינטרנט וספקי תוכן ופלטפורמות אינטרנטיות) ישירות נתוני תקשורת או חומר מחשב המאוחסן בשרתיהם או בענן.[73] נקודת המוצא לדיון שבמאמר זה היא בבקשת המדינה לבצע חדירה סמויה ומרחוק לחומר מחשב, היא פעולת הפצחנות. סעיף 23א(א) לפקודת סדר הדין הפלילי (מעצר וחיפוש) קובע כי "חדירה לחומר מחשב וכן הפקת פלט תוך חדירה כאמור, יראו אותן כחיפוש וייעשו על יד בעל תפקיד המיומן לביצוע פעולות כאמור".[74] לעניין זה החוק מגדיר חדירה

תפיסתם, אלא אם פנתה היחידה החוקרת לבית המשפט להארכת החזקת הציוד (שם, בסעיף 32(ב1)). תזכיר חוק סדר הדין הפלילי (סמכויות אכיפה – המצאה, חיפוש, כניסה ותפיסה), התשע"א–2011 (להלן: תזכיר חוק סדר הדין הפלילי, 2011) ביקשו לבטל את ייחודן של הוראות התפיסה של מחשב מוסדי לעומת מחשב רגיל לנוכח הקושי בהבחנה בין השניים בעידן הנוכחי והשימוש השכיח במחשב לשתי המטרת סימולטנית (פרטי ועסקי). ברע"פ 9446/16 **התובעת הצבאית הראשית נ' סיגאוי** (פורסם בנבו, 19.6.2017) נידונה השאלה, והושארה בצריך עיון, אם רשויות החקירה מוסמכות לערוך חיפוש במכשיר סלולרי (שתוכנו הוא חומר מחשב) על יסוד הסכמה של הנחקר ובלא היזקקות לצו שיפוטי.

[73] לעניין נתוני ההתקשרות ראו לדוגמה סעיף 11 לחוק שירות הביטחון הכללי, התש"ס–2002 וכן חוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), התשס"ח–2007. לעניין היכולת לדרוש חומר מחשב ישירות מספקי השירות, הסמכות מנויה בסעיף 23 לפקודת סדר הדין הפלילי (מעצר וחיפוש), המסמיך שופט בית משפט שלום "להזמין כל אדם" להמציא חפץ, אשר על פי ההנחה נמצא בהחזקתו או ברשותו של אדם, ואשר השופט מאמין כי הצגתו נחוצה או רצויה לצורכי חקירה או משפט. עם זאת ייתכן שחלק מהבקשות, כתלות בבקשה, כפופות לחוק האזנת סתר. לקריאה נוספת ראו: נמרוד קוזלובסקי **המחשב וההליך המשפטי: ראיות אלקטרוניות וסדרי דין** (תל אביב: לשכת עורכי הדין בישראל, 2000), עמ' 62. עוד ראו: כהנא ושני, לעיל ה"ש 68, בעמ' 34–42. לדיון באשר לסמכות זאת בראי פרשת **נטוויז'ן נגד צבא ההגנה לישראל**, ראו א' אינהורן ואח', **לוחמה בטרור בזירת המידע**, לעיל ה"ש 23, בעמ' 85. בספרות ובבתי משפט ברחבי העולם יש דיון ער בשאלת היקף יכולתן של מדינות לדרוש מחברות בין-לאומיות המספקות שירותי תוכן וגישה באינטרנט (רובן ככולן רשומות בארצות הברית, דוגמת גוגל, יאהוו!, מייקרוסופט, אמאזון, פייסבוק, טוויטר וכיו"ב) גישה הן לתוכן והן לנתוני ההתקשרות של משתמשיהם, שאותם הן שומרות על שרתיהן (מה שמכונה שירותי אחסון בענן). כך לדוגמה אם מכוח סעיף 43 לפקודת סדר הדין הפלילי המשטרה מוסמכת לדרוש ממייקרוסופט דוא"ל של אזרח ישראלי השמור בשרתים של החברה הממוקמים באירלנד. המורכבות של שאלות אלה היא תולדה של אופיו המיוחד של המידע כמושג שהוא במהותו א-טריטוריאלי, לעומת אופיו המיוחד של הדין כמושג שהוא במהותו טריטוריאלי. המתח אפוא קשור בשאלת סמכות השיפוט, התחולה החוץ-טריטוריאלית של הדין הישראלי, וחובות מקבילות החלות על החברות מכוח הדין הזר. לקריאה ראשונית בנושא ראו: Jennifer Daskal, *The Un-Territoriality of Data*, 125(2) YALE L. J. 326 (2015) וכן Andrew Woods, *Litigating Data Sovereignty*, 128(2) YALE L. J. 328 (2018).

[74] סעיף 23א(ב) לפקודת סדר הדין הפלילי (מעצר וחיפוש) [נוסח חדש], התשכ"ט–1969. בית המשפט המחוזי בת"פ (מחוזי י-ם) 2077/06 **מדינת ישראל נ' אריש**, תק-מח 2007(4) 10862 (2007) מצא כי לפחות בכל האמור בחיפוש בטלפונים סלולריים, יראו גם "בשוטר רגיל" או ב-"אדם סביר" "בעל תפקיד מיומן" העונה לדרישות הפקודה.

לחומר במחשב כמשמעותה בסעיף 4 לחוק המחשבים, כפי שנידון לעיל, קרי: חדירה באמצעות התקשרות או התחברות עם מחשב, או בהפעלתו.[75] אם נחזור להגדרת הנוזקה כפי שתוארה בפרק הקודם, נוכל בנקל לראות כיצד שימוש בנוזקה נופל בגבולותיו הרחבים של סעיף 4, בשים בצד את מתודת ההתפשטות הספציפית שבה תבחר היחידה החוקרת. כל רוגלה, תחייב בהכרח התקשרות או התחברות כלשהי אל המערכת כדי להזין אחורה אל החוקרים את המודיעין שנאסף ממנה.[76]

הפקודה מוסיפה עוד כי כל חיפוש שכזה תלוי בצו של שופט בית משפט שלום "המציין במפורש את ההיתר לחדור לחומר מחשב או להפיק פלט, לפי העניין, והמפרט את מטרות החיפוש ותנאיו שייקבעו באופן שלא יפגעו בפרטיותו של אדם מעבר לנדרש".[77] עם זאת ברור לכול כי סך המגבלות על פעילות רשויות האכיפה והביטחון המנויות בפקודה מצומצם בהרבה מזה המנוי בחוק האזנת סתר. מרחיבה על כך ד"ר אהרוני-גולנדברג, המבהירה כי "ככלל, בחוק האזנת סתר ישנם הליכים מחמירים יותר לקבלת צו שיפוטי ויחסית הוא מספק הגנה טובה יותר על סודיותו של המידע הממוחשב".[78] כך למשל לעומת צו האזנת סתר, הטוב רק לעבירות חמורות מסוג פשע, דיני החיפוש במחשבים אינם מוגבלים לרף עבירה ספציפי. יתרה מזאת, לעומת צו האזנת סתר, המאפשר פסילת ראיות ככלי לבקרה שיפוטית על החיפוש השלטוני, גם אם בדיעבד, באשר לראיות שהושגו בחיפוש במחשב שאינו כדין אלה "תהיינה קבילות בכפוף לדוקטרינת קבילות מצומצמת יותר שמקורה בפסיקה".[79] על אלה מוסיף ד"ר פוקס עוד הבדלים מהותיים. רשויות אכיפת החוק המבקשות צו חיפוש נדרשות ברף הוכחה נמוך יותר מבלי לבסס מהו טיב החומר שאותו הן מחפשות. "החוק אינו דורש שהחיפוש יהיה האמצעי האחרון, לאחר שאמצעים אחרים לא השיגו את המטרה.

---

[75] ראו לעיל, ה"ש 39.

[76] סעיף 99 לתזכיר חוק סדר הדין הפלילי, לעיל ה"ש 72, הציע תיקון לסעיף 4 שהיה מבהיר עוד יותר כי פעולות פצחנות באמצעות התקנת נוזקה נופלות בגבולות הסעיף. הנוסח המוצע קבע כי "חדירה לחומר מחשב הנמצא במחשב או בדבר המגלם חומר מחשב באמצעות התקשרות או התחברות עם מחשב או על ידי הפעלתו או על **ידי התקנה או חיבור של דברים המגלם חומר מחשב** או אמצעי אחסון של חומר מחשב" (ההדגשה שלי).

[77] סעיף 23א(ב) לפקודת סדר הדין הפלילי (מעצר וחיפוש).

[78] ראו: גולדנברג-אהרוני, לעיל ה"ש 38, בעמ' 480.

[79] שם.

החוק גם אינו מנחה את השופט לגבי השיקולים שעליו להתחשב בהם טרם אישור הבקשה״.[80]

עולה השאלה אפוא איזו מסגרת דינים תחול על פעולת פצחנות מצד גופי אכיפת חוק בישראל. רבות נכתב על המורכבות שבתיחום קווי הגבול שבין חוק האזנת סתר לפקודת סדר הדין הפלילי לעניין יירוט של מידע ממוחשב וחדירה אליו.[81] בדין הישראלי ניכרת הבחנה ברורה בין איסוף מידע מאוחסן (מידע המצוי במנוחה), אשר כפוף לפקודת סדר הדין הפלילי, לבין איסוף מידע מתקשורת בין מחשבים (מידע המצוי בתנועה), הכפוף ככלל לחוק האזנת סתר.[82] עם זאת קבלת מידע מתקשורת בין מחשבים, אגב חיפוש, מוחרגת מהעיקרון הכללי, וכן תכסה בצל הפקודה.[83] אם לא די בכך, סעיף 4 לחוק המחשבים מפריד בין ״חדירה לחומר מחשב״ לבין חדירה שהיא למעשה האזנה כמשמעה בחוק האזנת סתר.[84]

מה משמעותם של הדברים? התקנתה של רוגלה במחשב ואיסוף פסיבי של נתונים האגורים בו כפופים כולם למסלול המקל של הפקודה. זאת ועוד, גם איסוף בזמן אמת, אגב אותו חיפוש, של תקשורת בין מחשבים (לדוגמה: התכתובת דואר אלקטרוני או חילופי מסרים בוואטסאפ שמתקבלים במהלך החיפוש) יועתקו כדין, הגם שבמקור צו החיפוש התיר חיפוש במחשב ולא האזנת סתר לתקשורת בין מחשבים. כל פעולה נוספת במכשיר, בוודאי פעולות אקטיביות לשינוי המידע הממוחשב או שיבושו (לרבות הפעלת אפליקציות שונות, דוגמת המצלמה, המיקרופון, או האיכון הגאוגרפי), תחייב הצטיידות בצו להאזנת סתר ספציפית למטרה הספציפית. גזרה שווה אמורה לחול גם על איסוף פסיבי של תעבורה עתידית מאותו המכשיר, מלבד צו החיפוש הראשוני.[85] עם זאת אין זאת פרשנות מתחייבת. פעולת

---

[80] ראו: פוקס, לעיל ה״ש 68, עמ׳ 261.

[81] ד״ר פוקס מציין לדוגמה כי ״ההבחנה בין חיפוש לבין האזנת סתר אינה תמיד ברורה״, ראו: שם, עמ׳ 265. ד״ר אהרוני-גולדנברג, לדוגמה, מבקשת להימנע מהחלה בד בבד של הוראות החיפוש השונות בשני החוקים. במאמרה היא מתארת ״מסע וירטואלי״ של הודעה אלקטרונית בין שני מחשבים ומנסה להציע תיחומים שונים בכל אחד משלבי אותו מסע. ראו: גולדנברג-אהרוני, לעיל ה״ש 38, בעמ׳ 457–477.

[82] סעיף 1 לחוק האזנת סתר.

[83] סעיף 23א(ג) לפקודת סדר הדין הפלילי (מעצר וחיפוש).

[84] סעיף 4 לחוק המחשבים.

[85] ראו: גולדנברג-אהרוני, לעיל ה״ש 38, בעמ׳ 481–482.

הנוזקה עשויה להיות פעולה מתמשכת, ובהינתן האישור החוקי לאיסוף מידע מתקשורת בין מחשבים אגב החיפוש, ייתכן כי יש בכך להכשיר פעילויות איסוף רבות שבכל הקשר אחר היו נחשבות להאזנת סתר. בהקשר הזה קובעת גולדנברג-אהרוני, בהישענות על הפסיקה, כפי שמשתקפת בפרשת **פילוסוף**,[86] כי בכל מקום של ספק ראוי לאמץ סיווג פרשני מחמיר שלפיו כל אקט חיפוש ייחשב "האזנת סתר", שכן "מהבחינה העונשית ומבחינת הבקרה השיפוטית על החיפוש השלטוני, חוק זה מספק הגנה טובה יותר על חירויות אדם (קניין, אוטונומיה וחופש ביטוי) ועל הצורך התועלתני לאפשר שימוש חופשי במערכות מחשבים".[87]

מכל מקום, פקודת סדר הדין הפלילי קובעת כי מפכ"ל המשטרה הוא שנדרש לקבוע "הוראות נוספות לענין חדירה לחומר מחשב לצורך שמירה על הפרטיות ועל שלמותו של חומר מחשב". עוד מובהר כי הוראות אלה יכול שיעוגנו בפקודות משטרת ישראל או בנהלים פנימיים של המפכ"ל או של קצינים מטעמו.[88] אין בנמצא מידע שחשוף לציבור על נהלים אלו.

ב-2011 פורסם תזכיר חוק סדר הדין הפלילי (סמכויות אכיפה – המצאה, חיפוש, כניסה ותפיסה) שביקש להשלים את הסדרת דיני החיפוש והתפיסה של רשויות האכיפה בהליכים פליליים על בסיס המלצות ועדת לוין משנות התשעים.[89] התזכיר ביקש לייחד פרק נפרד, מחוץ להמלצות לוין, לפעולות אכיפה הנוגעות לחיפוש חומר מחשב ולחדירה אליו על רקע ההתפתחויות הטכנולוגיות שהתרחשו מאז דיוני הוועדה. ב-19.5.2014 עבר התזכיר כהצעת חוק בקריאה ראשונה. הן התזכיר והן

---

[86] ת"פ (מחוזי ת"א) 40206/05 **מדינת ישראל נ' פילוסוף**, תק-מח 2007(4) 9542 (2007) (המכונה גם פרשת הסוס הטרויאני, ועניינה פרשת ריגול עסקי שנחשפה בישראל בסוף המחצית הראשונה של שנת 2005. כחלק מהחקירה הורה פרקליט המדינה להפעיל את הליכי החיפוש במחשבים מכוח הפקודה ולא מכוח חוק האזנת סתר, אך בית המשפט המחוזי פסל את הראיות שהופקו בדרך זו, אגב יישומה של דוקטרינת פרי העץ המורעל).

[87] ראו: גולדנברג-אהרוני, לעיל ה"ש 38, בעמ' 481.

[88] סעיף 26(ב) לפקודת סדר הדין הפלילי (מעצר וחיפוש).

[89] במהלך שנות התשעים בחנה ועדה ציבורית בראשותו של שופט העליון בדימוס דב לוין את מכלול סמכויות האכיפה שבידי המשטרה – מעצר, חיפוש, הצגה, תפיסה וחילוט. בעקבות המלצותיה נחקקו חוק המעצרים, חוק החיפוש בגוף וחוק סמכויות לשם שמירה על ביטחון הציבור כפרקים להסדרת הסמכויות על בסיס המלצות הוועדה. חוק סדר הדין הפלילי (סמכויות אכיפה – מעצרים), התשנ"ו–1996, חוק סדר הדין הפלילי (סמכויות אכיפה – חיפוש בגוף ונטילת אמצעי זיהוי), התשנ"ו–1996 וחוק סמכויות לשם שמירה על ביטחון הציבור, התשס"ה–2005 נחקקו כפרקים להסדרת הסמכויות האמורות על בסיס המלצותיה של הוועדה.

הצעת החוק זכו לביקורת קשה מצד ארגוני חברה אזרחית. כך למשל הצעת החוק מבהירה כי קבלת מידע מתקשורת בין מחשבים אגב חיפוש לא תיחשב להאזנת סתר. כפי שמבהירה עו"ד אן סוציו, מנהלת תחום הזכויות בהליך הפלילי באגודה לזכויות האזרח, המשמעות היא כי המשטרה תוכל להתקין בעתיד רוגלות אשר יאפשרו לה מעקב אחר פעולות עתידיות של חשודים:

> "הסעיף יאפשר למשטרה להתקין תוכנה שמעבירה להם מידע מהטלפון, ולא רק למשוך את החומר עד אותו רגע – אלא גם לעתיד, לאסוף את המיילים שיקבל, את הודעות הווטסאפ, המיקומים וכדומה... הדבר דומה להתקנת מצלמה בביתו של אדם המבצעת מעקב על המתרחש בבית, תוך הארכת החיפוש לזמן בלתי מוגבל. דווקא בשל ההתפתחויות הטכנולוגיות, ההופכות את היקף החומר הנאגר לאדיר ממדים, נדרשת הקפדה יתרה על הזכות לפרטיות".[90]

ב-12.2.2018 החלו בוועדת החוקה, חוק ומשפט הדיונים לקראת הכנתה של הצעת החוק לקריאה שנייה ושלישית, אך הדיונים טרם הושלמו ויועברו לטיפולה של הכנסת העשרים ואחת. במגבלות מאמר זה אינני יכול להתייחס לתזכיר או להצעת החוק. עם זאת אבקש להקיש ממנו בכמה הזדמנויות, בפרק ד מטה עת אציע עקרונות מנחים להסדרה. כך או כך, בצל המגבלות התקציביות והטכנולוגיות של משטרת ישראל,[91] עיקר פעולות הפצחנות שמבצעות הרשויות אינן נחלת המשטרה. מבחינת היקף התקיפות, מבצעים אותן גופי הביטחון: השב"כ, המוסד ואגף המודיעין של צה"ל.

---

[90] זיו קריסטל, "מדינת משטרה? מבט לעתיד של חוק החיפוש החדש", **פוסטה: אתר לענייני חברה חוק ומשפט** 15.2.2018 https://posta.co.il/article/15916.

[91] ראו: אשד, לעיל ה"ש 69, בעמ' 604 ("בעיות קשות של תקציב, ובעיקר מדיור ושמירת טכנולוגיות רגישות עבור גופי המודיעין בעלי האוריינטציה הביטחונית, גרמו למשטרה לפתח בצורה יחסית את נושא הפעלת המקורות המודיעיניים האנושיים. המקורות הללו חיפו במידה רבה על הנחיתות העצומה בתחום הטכנולוגי"). ראו עוד: מבקר המדינה **דו"ח שנתי 67ב' לשנת 2016 ולחשבונות שנת הכספים 2015** "פרק שביעי: התמודדות משטרת ישראל עם פשיעת סייבר מתוחכמת" 1852–1853 (2017), (בין היתר מציין המבקר כי במועד הביקורת מנה תקן היחידה הארצית לטיפול בפשיעת סייבר כשליש בלבד מהיקף כוח האדם שנדרש לצורך התמודדות עם הנושא. עוד טוען המבקר כי ניכרים היעדר תקציב מספק ואי-הלימה בין הצרכים לרכש של ציוד טכנולוגי לצד קושי בגיוס מומחים רלוונטיים).

שניים מתוכם עסוקים במודיעין חוץ, אשר איננו מוסדר כלל בדין הישראלי.[92] האחרון, השב"כ, זכאי כזכור למסלול המקל של חוק האזנת סתר, שכן פעילותו חוסה בצל צורכי ביטחון המדינה. כך שבפועל, בהקשר של הרוב המוחלט של פעולות פצחנות שמבצעות הרשויות בישראל, הדין הקיים אומר מעט מדי ומגביל עוד פחות.[93]

1.ב. התיקון המוצע לחוק השב"כ

הצעת חוק המאבק בטרור, התשע"א-2011 כללה כלים רבים מתחומי המשפט הציבורי והפלילי אשר נועדו לאפשר למדינת ישראל להיאבק בארגוני טרור ולסכל עבירות טרור באפקטיביות בתוך כדי איזון עם מחויבויותיה של מדינת ישראל "לזכויות האדם ולאמות המידה המקובלות בתחום זה במשפט הבין-לאומי".[94] אחד מן הכלים שעלו בהצעה הוא סעיף 131 שעניינו תיקון לחוק השב"כ אשר מסמיך את השירות במפורש לבצע תקיפות מחשבים למטרות סיכול של פעילות טרור או ריגול נגד מדינת ישראל.[95] כפי שנכתב בדברי ההסבר להצעה, על רקע התגברות פעילויות טרור והסתה לטרור המשתמשות בטכנולוגיה מתקדמת מתחום המחשבים, יש "צורך חיוני" במתן סמכות מפורשת לשב"כ לבצע "פעולות בחומר מחשב".[96] נציג השב"כ

---

[92] כהנא ושני, לעיל ה"ש 68, בעמ' 275–276 (כהנא ושני מבהירים כי "מאחר שמעמדו של המוסד לתפקידים מיוחדים טרם הוסדר בחקיקה, אין פלא שכאשר מסורות בידיו אי אילו סמכויות מעקב אחר רשתות תקשורת, הדין הישראלי שותק. ואולם גם באשר לפעילותם של שירות הביטחון הכללי, אגף המודיעין במטה הכללי ומשטרת ישראל מתעוררות שאלות שלמותר ואסור בנוגע לתקשורת זרה וליעדים מודיעיניים זרים, לרבות הבחנות דקות יותר באשר להוראות החלות על מעקב מקוון שיעדיו הם תושבי שטחים שבשליטת ישראל. נדרשת אפוא הסדרה מלאה ופרטנית של היקף הסמכויות של כל אחד מגופי הביטחון ואכיפת החוק השונים – הן מבחינת הפרקטיקות המותרות להם, היקף האיסוף המותר והבקרות המופעלות עליהן והן מבחינת ההיקף הטריטוריאלי/פרסונלי של סמכויות אלו").

[93] ראו עוד: קוזלובסקי, לעיל ה"ש 73, בעמ' 54 ("הוראות הדין חסרות יסודות חיוניים החייבים להמצא בהוראות המסדירות את הסמכות לחפש אצל הפרט ואינן נותנות כלים מנחים בידי רשויות אכיפת החוק ובתי המשפט לעניין דרך ביצועו של חיפוש מעין זה") וכן כהנא ושני, לעיל ה"ש 67, בעמ' 52–54).

[94] סעיף 1 לחוק המאבק בטרור.

[95] סעיף 131 להצעת חוק המאבק בטרור.

[96] דברי ההסבר להצעת חוק המאבק בטרור, 1492.

בדיונים הוסיף כי "החוק שאנו עובדים איתו היום, מתאים לאיומים שהיו לפני 50 שנה ולא לעידן הטכנולוגי והרשתות החברתיות".[97]

בשל מורכבות ההצעה החליטה ועדת החוקה, חוק ומשפט של הכנסת בתאריך ה-28.3.2016 לפצל מהצעת החוק את סעיף 131 כדי לאפשר דיון פרטני בסעיף בוועדה במנותק מהחוק הכולל.[98] לפיכך חוק המאבק בטרור, אשר עבר בקריאה שלישית ביוני 2017, נמנע מהעיסוק בשאלת סמכויות גורמי אכיפת החוק לביצוע פעילויות חקירה במרחב הקיברנטי. נכון לדצמבר 2019 טרם נתקיים הדיון בוועדה על סעיף 131 המפוצל. דיון שכזה, אשר היה אמור להתקיים במהלך 2018-2019, נדחה לבינתיים עד השבעתה של הכנסת ה-23, וייתכן כי הדיון בו ייעשה בד בבד עם הדיונים בדבר חדירה לחומר מחשב לפי הצעת חוק החיפוש שאוזכרה לעיל.

ההסדר שהוצע בסעיף 131 ביקש לשכפל, בכפוף לשינויים המחויבים, את ההסדרים הנוגעים להאזנות סתר למטרות ביטחון המדינה כפי שהם מנויים בחוק האזנת סתר וליישמם בפעולות פצחנות של השב"כ. על פי ההצעה, ראש הממשלה, לבקשת ראש השירות, יהיה רשאי להתיר בעצמו וללא צו פעולה סמויה במחשבים או בחומרי מחשב בתנאי ששוכנע כי "הפעולה חיונית למטרות סיכול או מניעה של פעילות טרור או ריגול שיש בהם משום סיכון חיי אדם או פגיעה חמורה בביטחון המדינה וכי לא ניתן, באופן סביר, להשיג את המטרה האמורה בדרך אחרת". עוד נקבע בהסדר כי במקרים חיוניים, שאינם סובלים דיחוי, יהיה ראש השירות רשאי לבדו להתיר בכתב תקיפות כאמור, בתנאי שידווח על כך מייד לראש הממשלה. ההסדר מונה שני מנגנונים אשר נועדו להבטיח שימוש "זהיר ומידתי" בסמכות האמורה: ראשית ההסדר מציע לתחום בזמן את תקופת תוקפם של ההיתרים האמורים (עד 30 יום להיתר שנתן ראש הממשלה, ועד 48 שעות להיתר שנתן ראש השירות); שנית קובע

---

[97] חדשות ועדת החוקה, חוק ומשפט "נציג השב"כ בדיון בחוק המאבק בטרור – החוק שאנו עובדים איתו היום, מתאים לאיומים שהיו לפני 50 שנה" **אתר הכנסת** 12.10.2015 goo.gl/AFaag6.

[98] פרוטוקול ישיבה מס' 120 של הכנסת ה-20, 217 (28.3.2016) (ניסן סלומינסקי, יו"ר וועדת החוקה, חוק ומשפט: "על-פי הצעת ועדת החוקה, חוק ומשפט של הכנסת, מחליטה הכנסת, לפי סעיף 84ב לתקנון הכנסת, לאשר את החלטת ועדת החוקה, חוק ומשפט לפצל את הצעת חוק המאבק בטרור, התשע"ה–2015, לשתי הצעות חוק נפרדות, כך שחלק אחד מההצעה יכלול את סעיפים 115, 120, 131, וכן פסקה (2) בסעיף 42 המוצע בסעיף 130, וחלק אחר מההצעה יכלול את יתר הצעת החוק. אני פונה לחברי ומבקש לאשר את הפיצול, כדי שנוכל לסיים כפי שסיימנו את חוק המאבק בטרור, ונושא נוסף יישאר לנו להמשך").

ההסדר כי כשמדובר בחומר מחשב המשמש עורך דין, רופא, פסיכולוג, עובד סוציאלי או כהן דת, תותר פעילות החדירה, בדומה להאזנת סתר, רק בצו בית משפט (לבד מבמקרים שאינם סובלים דיחוי, אז יותר לראש השירות לאשר לבדו גם תקיפות שכאלה, אך בכפוף לדיווח ליועץ המשפטי לממשלה אשר יהא מוסמך לבטל את ההיתר).[99]

בשארית מאמר זה אני מבקש לעמוד על השאלה אם האיזונים המגולמים בסעיף 131 המפוצל עולים בקנה אחד הן עם דיני זכויות האדם הבין-לאומיים והן עם "אמות המידה המקובלות בתחום זה במשפט הבין-לאומי", כמתבקש מלשון סעיף 1 לחוק המקורי. כדי להשיב על שאלה זו אדרש תחילה לכללי המשפט הבין-לאומי החלים בענייננו ולאחר מכן אבחן את הדין הזר בארבע מדינות שונות: שתי מדינות מהמשפט המקובל (ארצות הברית ואנגלייה) ושתי מדינות מהמשפט הקונטיננטלי (צרפת ואיטליה).

2. הדין הבין-לאומי

במשפט הבין-לאומי אין הסדרה מפורשת של פעולות פצחנות למטרות שיטור ואכיפת חוק, וודאי שלא כחלק מפעולות ביון וריגול חוצות-גבולות.[100] עם זאת ניכרת

---

[99] הצעת חוק המאבק בטרור, 1492–1494.

[100] בספרות קיים ויכוח עקרוני בשאלה אם פעולות פצחנות חוצות-גבולות למטרות אכיפת חוק המבוצעות בלא ידיעת או הסכמת המדינה המותקפת עולות לכדי הפרה של חזקת אי-התחולה החוץ-טריטוריאלית המעוגנת במשפט הבין-לאומי (The Presumption Against Extraterritoriality) או האיסור על הפעלת סמכות אכיפה מחוץ לגבולות המדינה כפי שקבע בית הדין הבין-לאומי לצדק בפרשת לוטוס (וראו: *S.S. Lotus (Fr. v. Turk.)*, Judgment, 1927 (ser. A) No. 10 (Sept. 7) (שם נקבע כי "the first and foremost restriction imposed by international law upon a State is that – failing the existence of a permissive rule to the contrary – it may not exceed its power in any form in the territory of another State. In this sense jurisdiction is certainly territorial; It cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom or from a convention"). לדיון נוסף ראו מטה בה"ש 115 ו-117. באשר לפעולות פצחנות חוצות-גבולות למטרות ריגול וביון נסב הדיון ככלל על השאלה אם יש לראות בריגול כשלעצמו פעולה אסורה או מותרת על פי המשפט הבין-לאומי הפומבי. סוגיה מורכבת זו איננה יכולה לזכות לדיון מספק בגבולות רשימה זו. לקריאה נפרדת

בשנים האחרונות מגמה בקרב סוכנויות או"ם וגופים מומחים לזכויות אדם לפיתוחן של נורמות רכות סביב חוקיות השימוש בכלי פצחנות כחלק מדיני זכויות האדם הבין-לאומיים. הראשון להשמיע גישה זו היה הדווח המנחה לזכות לחופש הביטוי פרנק ויליאם לה רו שציין בחוות דעתו מ-2013 כי פעולות פצחנות אינן רק כלי טכנולוגי חדש לריגול כי אם דרך חדשה של ריגול. לאור זאת מנקודת מבט של זכויות אדם, השימוש בכלים אלו "מטריד במידה קיצונית".[101]

ראו: Asaf Lubin, *The Liberty to Spy*, 61(1) HARVARD INT'L. L. J. (forthcoming, 2019). ככלל, קבוצת המומחים הממשלתיים של האו"ם קבעה ב-2015 כי על מדינות להימנע מהשמשתם של שירותי תקשורת אשר עלולים לגרום נזק או להציב סיכון לסדר והביטחון הבין-לאומיים (וראו: U. N GAOR, 70th Sess., at U.N. Doc. A/70/174 (Jul. 22, 2015). https://undocs.org/A/70/174

[101] ראו: U. N GAOR, 23th Sess., at U.N. Doc. A/HRC/23/40 (Apr. 17, 2013).: https://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Sessio n23/A.HRC.23.40_EN.pdf

Offensive intrusion software such as Trojans, or "mass interception capabilities, constitute such serious challenges to traditional notions of surveillance that they cannot be reconciled with existing laws on surveillance and access to private information. There are not just new methods for conducting surveillance; they are new forms of surveillance. From a human rights perspective, the use of such technologies is extremely disturbing. Trojans, for example, not only enable a State to access devices, but also enable them to alter – inadvertently or purposefully – the information contained therein. This threatens not only the right to privacy but also procedural fairness rights with respect to the use of such evidence in legal proceedings"). ראו עוד: דוח הדווח המנחה לזכות לפרטיות, ממארס 2016, שם טען בהקשר של חוק ה-IPA, טרם אישורו כי על ועדות הפרלמנט הבריטי לפעול: " with renewed vigour and determination, to exert their influence in order that disproportionate, privacy-intrusive measures such as bulk surveillance and bulk hacking as contemplated in the Investigatory Powers Bill be outlawed rather than legitimized… the UK Government [should] how greater commitment to protecting the fundamental right to privacy of its own citizens and those of others and also to desist from setting a bad example to other states by continuing to propose measures, especially bulk interception and bulk hacking, which prima facie fail the standards of several UK Parliamentary Committees, run counter to the most recent judgements of the European Court of Justice and the European Court of Human Rights, and undermine the spirit of the very right to privacy". ראו: U.N Secretary-General, Report of the Special Rapporteur on the Right to Privacy, Rep. of the Secretary-General, U.N. Doc. A/HRC/31/64, para. 39 (Nov. 24, 2016).

גישה דומה אימצו גופי אמנה. ישראל היא צד לאמנה לזכויות אזרחיות ופוליטיות ומחויבת לפרשנות המקובלת לזכויות האמונות בה, לרבות הזכות לפרטיות המעוגנת בסעיף 17 לאמנה. במארס 2017 התייחסה הוועדה לזכויות האדם של האו"ם, הגוף האמון על פרשנות ויישום האמנה לזכויות אזרחיות ופוליטיות, כתקדים, לשימוש בכלי פצחנות מצד גופי אכיפה וביון בהקשר של הדוח התקופתי של איטליה. הוועדה ציינה כי היא מוטרדת מהדיווחים שלפיהם רשויות אכיפת החוק באיטליה משתמשים "בכלי פצחנות" בהיעדר הרשאה סטטוטורית מפורשת ובלי לקבוע אמצעי ביטחון מפני ניצול לרעה של הכוח. הוועדה קבעה עוד כי פעולות פצחנות מסוג אלה חוסות בצל סעיף 17 לאמנה המגן על הזכות לפרטיות, וכי על איטליה לעמוד בדרישות המשפטיות שהסעיף מקים עליה. לפיכך נתבקשה איטליה להכפיף את פעילות הפצחנות שלה לעקרון החוקיות, הנחיצות והמידתיות, לרבות על דרך של אימוצם של מנגנונים עצמאיים לביקורת מראש ובדיעבד אחר פעילות הפצחנות וכן יצירת נהלים לדיווח על פעולות פצחנות למי שהיו מטרות התקיפה ומתן הזדמנות שווה להם לדרוש שיפוי מקום שזכויותיהם הופרו.[102]

הגישה הרווחת אפוא מבקשת לראות בפעולות פצחנות מצד גופי אכיפת חוק וביון פעולת מעקב ככל פעולת מעקב אחרת, ולפי זה להכפיף אותן לפסיקה ולספרות הקיימת בדיני זכויות האדם בדבר פעולות מסוג אלה. כפי שמרחיב פרופ' יובל שני, הנשיא הנוכחי של הוועדה לזכויות האדם של האו"ם, הוועדה מפרשת את האיסור על "שרירותיות" המנוי בסעיף 17 לאמנה לזכויות אזרחיות ופוליטיות כדרישה רחבה הגוזרת אלמנטים של סבירות, נחיצות ופרופורציונליות לצד דרישות של מנהל תקין, צפיות ומניעת אי-צדק.[103] פסיקת בית הדין האירופי לזכויות אדם ובית הדין האירופי לצדק בדבר הזכות לפרטיות והזכות להגנת מידע משקפת גישה דומה הקובעת גבולות לכוחה של המדינה להפעיל אמצעי מעקב והאזנה הן בשטחה והן מחוץ לשטחה.

---

[102] U.N Secretary-General, Concluding Observations on the Sixth Periodic Report of Italy, Human Rights Committee, Rep. of the Secretary-General, U.N. Doc. CCPR/C/ITA/CO/6, paras. 36-37 (May. 1, 2017) (להלן: דוח הוועדה לזכויות האדם של האו"ם בעניין איטליה).

[103] ראו, יובל שני " On-Line Surveillance in the case-law of the UN Human Rights Committee" **מרכז המחקר להגנת סייבר באוניברסיטה העברית בירושלים** 13.7.2017 https://csrcl.huji.ac.il/people/line-surveillance-case-law-un-human-rights-committee?ref_tid=3718.

ניתן אפוא לסכם את עיקרי הפסיקה והספרות בשבעה עקרונות מרכזיים, כאשר כל אחד מהם כולל בחובו של עקרונות משנה. עקרונות אלה משקפים במידה רבה גם את החקיקה במרבית המדינות המערביות, וייתכן כי הם מבטאים מגמה לקראת קודיפיקציה של דין מנהגי מחייב.[104]

1. **עקרון החוקיות**: הגוזר את החובה להסמיך בחקיקה ראשית את גופי הביון ואכיפת החוק לביצוע פעולות מעקב. כנגזרת של עקרון החוקיות מוכרים בפסיקה שני עקרונות משנה: (א) עקרון הגישה (accessibility) המחייב לאפשר גישה נוחה לציבור הרחב באשר להסדרים הקיימים; (ב) עקרון הצפיות (foreseeability) המחייב כי הפרוצדורות הקבועות בחוק יהיו ספציפיות וברורות דיין כדי לבאר את מסגרת הנסיבות שבשלה עשוי אדם למצוא את עצמו בפעולת מעקב.
2. **עקרון הנחיצות**: המחייב למנות בחוק את המטרות המצדיקות פעולת מעקב ספציפית ולהדגים קיומו של קשר רציונלי בין האמצעים הקבועים בחוק לבין המטרות כאמור.
3. **עקרון הפרופורציונליות**: הכולל בחובו הן מבחן הפגיעה הפחותה (הגורס כי בטרם אישור הפעולה ייבחנו מעשית אמצעים שפגיעתם בזכויות אדם פחותה) ומבחן המידתיות במובן הצר (הפוסל פעולת מעקב מקום שהפגיעה בזכויות אדם היא ללא יחס ראוי לתועלת שהיא מביאה בהגשמת התכלית).
4. **עקרון האישור המקדים (ex ante authorization)**: דרישה לאישור מקדים של הרשות השופטת, או למצער המבצעת, לכל פעולת מעקב. בתהליך האישור יש לבחון לעומקם את עקרונות הנחיצות, הפרופורציונליות ואמצעי

---

[104] באוגוסט 2017 פרסם ארגון Privacy International מורה נבוכים בדבר כללי המשפט הבין-לאומי שחלים בהקשר של פעולות מעקב. הנייר כולל בתוכו מאות ציטוטים מן הפסיקה המעגנים את כל אחד מן העקרונות המובאים מטה. ראו: Guide to International Law and Surveillance, PRIVACY INTERNATIONAL (Sep. 2017), https://privacyinternational.org/long-read/993/guide-international-law-and-surveillance-20.

הביטחון ולאשר פעולות רק על בסיס של "חשד סביר" ומכוח בחינה פרטנית של הנסיבות.

5. **עקרון אמצעי הביטחון (safeguards from abuse)**: הכולל פרוצדורות למזעור נזקים אפשריים (minimization procedures). הפניה אחת, המוכרת בספרות, היא ל-Weber 6, הכוונה היא לשישה כללים שנקבעו בפרשת *Weber and Saravia v. Germany* של בית הדין האירופי לזכויות אדם.[105] ככלל מדובר במגבלות הנוגעות לאופן איסוף המידע ואגירתו, הגישה אליו, שיתופו עם גורמים שלישיים ומחיקתו. על אלה יש להוסיף עקרונות הנוגעים להגנה על השרשרת הראייתית, לצמצום איסוף "מידע אגבי" ולהגנה על מידע רגיש (בדגש על מידע הכפוף לחיסיון כדין).

6. **עקרון השקיפות, הבקרה והפיקוח המאוחר (ex post review)**: הדרישה לפיקוח עצמאי ואפקטיבי מצד ישות (משפטית, אדמיניסטרטיבית או פרלמנטרית) בעלת גישה מלאה ואמצעים כדי לעודד שקיפות וחשיפה ולצמצם את הסיכון לניצול לרעה של סמכויות.

7. **עקרון היידוע והשיפוי**: לבסוף מעוגנת הדרישה ליידע קורבנות מעקב במועד הראשון האפשרי מבלי לפגוע בצורכי החקירה. כמו כן יש לאפשר גישה לערכאות גם למי שאינם יכולים להוכיח בוודאות כי אכן ריגלו אחריהם (הליכי *in abstracto*) ולאפשר שיפוי ותרופה במקרה שהוכח ניצול לרעה או שלא כדין של הסמכויות האמורות.

---

[105] ראו: Weber and Saravia v. Germany, App. No. 5493/00 , 2006-III Eur. Ct. H. R. at 95 (שם נקבע כי: "In the case-law on secret measures of surveillance the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed").

3. הדין המשווה

בראי עקרונות אלה המאמר ממשיך לסקור את מסגרת הדין הנוגעת לפעולות פצחנות באמצעות מנגנוני ביון ואכיפת חוק בדין האמריקאי, האנגלי, הצרפתי והאיטלקי. מתוך סקירה משווה זו ייגזרו המלצות מדיניות לרשות המחוקקת בבואה לבחון אם לאמץ את התיקון המוצע לחוק השב"כ (ואגב כך גם את הצעת חוק סדר הדין הפלילי (סמכויות אכיפה – המצאה, חיפוש ותפיסה), התשע"ד–2014)). יודגש כי בכל האמור בפעילות פצחנות מצד גורמי שיטור, ביון ואכיפת חוק במדינות שונות רב הנסתר על הגלוי. לפיכך מתעורר קושי לנסות לבאר בדיוק מהן הסמכויות הקבועות בדין בכל מדינה ומדינה, ומהם הכלים הזמינים לרשויותיה בקידום פעולות מודיעיניות כחלק מהמאבק בפשיעה החמורה, בטרור ובריגול עוין. בתהליך הכתיבה שאפתי לנסות ולסדר את פרקי המשפט המשווה בחלוקה לתתי-נושאים. עם זאת מידע אשר זמין בעניין מסוים על מדינה אחת איננו בהכרח זמין על מדינה אחרת. לכן התעורר קושי להציע חלוקה סדורה ותבניתית שתחזור על עצמה בין המדינות ותסייע לקורא בהשוואה. עם זאת פרק זה יסתיים בסיכום שאני מקווה שיוכל להבהיר מהם ההבדלים בין המדינות, ומהם האיזונים שכל מדינה עשתה בראי הדין שלה.

3.א. הדין האמריקאי

3.א.1. רקע היסטורי

המקרה הידוע הראשון של שימוש בפעולות פצחנות מצד גופי אכיפת חוק בארצות הברית התרחש בשנת 1999. בינואר אותה שנה פשטו סוכני לשכת החקירות הפדרלית על משרדו של בוס מאפיה בשם "ניקי הקטן" סקארפו ומצאו בו מחשב. הם העתיקו את תוכן הדיסק הקשיח שלו, אבל לא היו יכולים לקרוא את המסמכים שנשמרו בו, מכיוון שאלה קודדו באמצעות תוכנת PGP (Pretty Good Privacy). הסוכנים קיוו למצוא ראיות מפלילות נגד משפחת המאפיה גמבינו. באביב שבו סוכני ה-FBI למשרד כשבידם צו חיפוש מבית משפט והתקינו בחשאי במחשבו האישי של ניקודמו סקארפו, בנו של "ניקי הקטן", תוכנה מסוג "רושם הקשות" (Key Logger).

באמצעות התוכנה הצליחו לאתר סיסמה שסייעה בשחרור ההצפנה ובכך נחשפו למסמכים אשר הפלילו הן את סקארפו הבן והן את סקארפו האב בכמה וכמה עבירות של ניהול בתי הימורים והלוואות לא חוקיות. הגם שסקארפו ניסה להעלות טענת "הפרי המורעל", פסק שופט פדרלי בניו-ג'רזי לבסוף לטובת המדינה והתיר השימוש בראיות שנאספו.[106]

לעומת הפרשה הראשונה, שבה נדרשו סוכני לשכת החקירות להתקין בעצמם את התוכנה במחשב, פרשת תיכון טימברליין כבר כללה שימוש בנוזקה וגישה מרחוק. במאי–יוני 2007 קיבל תיכון טימברליין במדינת ושינגטון כמה אזהרות שווא בדבר קיומה של פצצה בשטחי בית הספר. בכל פעם פונו התלמידים והצוות מהזירה, וכוחות הביטחון המקומיים נדרשו למקום. האזהרות הגיעו כדוא"לים משרת לא מזוהה באיטליה. לא זו אף זו, ב-4 ביוני אף הותקפה רשת המחשבים של מחוז בתי הספר לייסי בתקיפת מניעת שירות והביאה לקריסתם. כחלק מחקירתם איתרו סוכני ה-FBI שם משתמש בפלטפורמת timberlinebombinfo – My Space. מכוח צו בית משפט התחזו הסוכנים לעיתונאים ושלחו הודעה לשם המשתמש בפלטפורמה. ההודעה כללה קישור פיקטיבי שלחיצה עליו התקינה מערכת בשם "מזהה כתובות פרוטוקולי אינטרנט ומחשבים" (או CIPAV בקיצור). בבקשה לצו טענו בפני השופט כי CIPAV תסייע להם לזהות את מערכת ההפעלה של החשוד, את כתובת ה-IP שלו, כתובת ה-MAC שלו, מידע על המחשב, על הדפדפן ועל היסטוריית הגלישה שלו. השימוש בתקיפת "הנדסה חברתית" היה אפקטיבי, והרוגלה הותקנה במחשבו של החשוד, תלמיד בן 15 מתיכון טימברליין. בדיעבד התברר כי הרוגלה פעלה במחשבו של התלמיד למשך 60 ימים.[107]

---

[106] ראו: ג'ון שוורץ "ביהמ"ש יכריע: האם אפשר לפרוץ למחשב ללא צו" **הארץ** 31.7.2001 https://www.haaretz.co.il/misc/1.722405.

[107] לקריאה נוספת על האירוע ועל תקיפות מחשבים נוספות שהתרחשו בארצות הברית בתקופה האמורה מצד לשכת החקירות הפדרלית, ראו: Sayako Quinlan & Andi Wilson, *A Brief History of Law Enforcement Hacking in the United States*, NEW AMERICA (Sep. 2016), https://na-production.s3.amazonaws.com/documents/History_Hacking.pdf .

3.א.2. המסגרת החוקית לפעילות פצחנות מודיעינית מצד גופי השיטור

נראה כי מאז 1999 ועד היום הבסיס החוקי לפעולות פצחנות בשטח ארצות הברית מעוגן בדין האמריקאי בסעיף 41 לכללי סדר הדין הפלילי הפדרליים שעניינו סמכות חיפוש ותפיסה.[108] במיוחד רלוונטי הכלל שלפיו שופט מחוזי רשאי להורות בשטח המחוז, ובהקשר של עבירות טרור גם מחוץ לשטח זה, על התקנה של "אמצעי איכון" כדי לעקוב אחר תנועותיו של אדם או של חפץ (גם אם אותו אדם או חפץ יצאו לאחר מכן מחוץ לשטח המחוז).[109] נראה כי עד דצמבר 2016 אושרו מכוחו של הכלל הזה וגם נדחו בקשות לצווים להתקנת נוזקות כחלק מחקירות פדרליות.[110]

בדצמבר 2016 נכנס לתוקפו תיקון לסעיף 41 שהוצע במקור במשרד המשפטים האמריקאי ואושר בבית המשפט העליון האמריקאי.[111] התיקון עיגן לראשונה במפורש את הסמכות של בתי המשפט להורות בצו על קידום "טכניקות חקירה רשתיות" (Network Investigative Techniques או NIT בקצרה). התיקון מקנה

---

[108] לקריאה נוספת ראו: Policy Department, Citizens' Rights and Constitutional Affairs, *Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices*, EUR. PARL. DOC. PE 583.137, pp. 121-122 (2017). http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf (להלן: מחקר הפרלמנט האירופי).

[109] ראו: FED. R. CRIM. P. 41 (ראו שם בסעיף (b)(4) נכתב: "a magistrate judge with authority in the district has authority to issue a warrant to install within the district a tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both").

[110] כך לדוגמה ב-2013 במחוז הדרום של טקסס סירב שופט להעניק צו לתקיפת מחשב אשר על פי החשד שימש לביצוע עבירות הונאה, בטענה כי גם זהות בעלי המחשב וגם מיקום המחשב לא היו ידועים במועד הגשת הבקשה. לפיכך חשש השופט כי אישור הבקשה יהא כרוך בהפרת גבולותיה הטריטוריאליים של סמכות השיפוט שלו. ראו: Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753 (S.D. Tex. 2013).

[111] מכוחו של ה-Rules Enabling Act התיקון לסעיף 41 אושר בבית המשפט העליון האמריקאי ב-28 באפריל 2016 והובא לידיעת הקונגרס. התיקון נכנס לתוקפו ב-1 בדצמבר 2016. וראו: https://www.supremecourt.gov/orders/courtorders/frcr16_mj80.pdf.

לשופט מחוזי את הסמכות לאשר בצו "גישה מרחוק" למדיה אלקטרונית המצויה מחוץ לסמכות שיפוטו, בהתקיים אחד משני התנאים האלה:[112]

(א) מיקום המדיה או המידע הוסתר באמצעים טכנולוגיים.

(ב) בחקירת עבירות סייבר, כאשר הושמש מערך רובורשת הנפרס על פני חמישה תחומי שיפוט או יותר.[113]

בפועל נועד התיקון לסייע במאבק בפשיעת סייבר, בייחוד כשזו מתבצעת בשימוש בכלי אנונימיזציה רשתיים וברשת האפלה. הדוגמה המועלית בספרות בהרחבה נוגעת לפרשת אתר Playpen. מדובר באתר אינטרנט ברשת האפלה אשר נתן גישה לפורנוגרפיית ילדים. בפברואר 2015 תפסו ה-FBI את שרתי האינטרנט אך במקום לסגור אותם המשיכו להפעילם למשך 13 ימים מכוח צו של השופטת טריסה ביוקנן הפועלת מהמחוז המזרחי של וירג'יניה. החוקרים השתמשו בתקיפת באר מים, וכך כל משתמש שהוריד תוכן מהשרת קיבל אל מחשבו גם נוזקת ריגול אשר סיפקה לחוקרים, חרף שרתי האנונימיזציה, מידע מדויק על מיקומו של הגולש ואת פרטיו. התיקון לחוק נועד להבטיח שצו מהסוג שאישרה השופטת ביוקנן יהיה קביל גם בעתיד.[114]

---

[112] ראו: FED. R. CRIM. P. 41 (ראו שם בסעיף (b)(6)): "a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if: A) the district where the media or information is located has been concealed through technological means; or B) in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts").

[113] סגנית התובע הכללי לזלי קולדוול פרסמה בלוג קצר ובו דברי הסבר לתיקון. ראו: Lesley Caldwell, *Rule 41 Changes Ensure A Judge May Consider Warrants for Certain Remote Searches*, DEPARTMENT OF JUSTICE (Jun. 20, 2016) https://www.justice.gov/archives/opa/blog/rule-41-changes-ensure-judge-may-consider-warrants-certain-remote-searches.

[114] לקריאה נוספת ראו: סוכנויות הידיעות, "הבולשת הפדרלית בארצות הברית הפעילה אתר פורנו ילדים; תנועת הגולשים לאתר זינקה פי חמישה" **דה מרקר** 28.9.2016 https://www.themarker.com/wallstreet/1.3082912.

3.א.3. דיון ביקורתי

פרופ' גאפור מעלה ביקורת קשה על התיקון וטוען כי הוא מסכן את יחסי החוץ של ארצות הברית. היות שצו אחד מאפשר תקיפה של מאות אם לא אלפי מחשבים לא מזוהים, הוא עשוי להוביל להפעלת סמכות שיפוט חוץ-טריטוריאלית.[115] אכן בפרשת "Plaype" הותקפו לא פחות מ-8,000 מחשבים ביותר מ-120 מדינות.[116] כפי שמרחיב גאפור, התיקון מייצר מצב שבו הדרגים הנמוכים ביותר ב-FBI זוכים לשיקול דעת נרחב המאפשר להם לעצב את מדיניות-החוץ והסייבר של ארצות הברית.[117]

על פי הדיווח, סוכני הבולשת אף דאגו לשפר ולשדרג את חוויית הגלישה ואת מהירותה, ובכך הגדילו את שיעור המשתמשים בתקופה האמורה. משרד המשפטים האמריקאי הגיש קרוב ל-200 אישומים נגד אזרחים אמריקאים בעקבות החקירה. רבים מהם ביקשו לפסול את הראיות, שכן הצו אושר בטרם התיקון לחוק, ולכאורה חרגה השופטת מסמכותה באפשרה תקיפות מחשבים מחוץ לסמכות השיפוט שלה. בכל המקרים עד כה סירבו בתי המשפט לקבל את טענת החריגה מסמכות, או קיבלו אותה אך סירבו לפסול את הראיות מכוח חריג תום הלב. לקריאה נוספת ראו: Susan Hennessey, *The Elephant in the Room: Addressing Child Exploitation and Going Dark*, HOOVER INSTITUTION ESSAY, 15 (Jan. 27, 2017), https://www.hoover.org/sites/default/files/research/docs/hennessey_webreadypdf.pdf ("As of November 2016, judges in more than twenty-five federal districts had presided over matters relating to a Playpen prosecution. A primary issue in these cases was whether the warrant, obtained in the Eastern District of Virginia, violated Rule 41 when applied to computers outside that district. Although courts diverged significantly in their analyses and conclusions,85 a majority of courts found that the warrant at least technically violated Rule 41 but relied on the good-faith exception in declining to suppress evidence").

[115] ראו: Ahmed Ghappour, *Searching Places Unknown*, 69(4) STANFORD L. REV. 1075 (2017).

[116] לקריאה נוספת ראו: Joseph Cox, *The FBI Hacked Over 8,000 Computers in 120 Countries Based on One Warrant*, MOTHERBOARD (Nov. 22, 2016), https://www.vice.com/en_us/article/53d4n8/fbi-hacked-over-8000-computers-in-120-countries-based-on-one-warrant.

[117] ראו: גאפור, לעיל ה"ש 115, בעמ' 1108 ("rank-and-file officers have discretion that may shape U.S. policy regarding which crimes trigger the use of crossborder network investigative techniques, the breadth of hacking techniques that are used

לפיכך מציע גאפור כמה וכמה המלצות לשיפור המסגרת הקיימת בארצות הברית לפעולות פצחנות למטרות אכיפת חוק, הן מבחינה רגולטורית והן מבחינה פרקטית.[118] ראשית הציע גאפור שיתוף פעולה בין-משרדי ובין-ארגוני לטובת גיבוש של כללים מנחים לפעולות פצחנות מצד ה-FBI כדי להבטיח שמדיניות הארגון תהיה גמישה מספיק להתמודד עם שינויים בזירת הסייבר וכן תוביל להגדלת שיתוף הפעולה והיקף המומחיות של הארגון בביצוע פעולות אלה.[119] בין היתר הציע גאפור כי שימוש בכלי תקיפה מסוימים, בעלי רגישות מיוחדת, יוגבל.[120]

שנית קבע גאפור כי פעולות פצחנות נגד יעדים לא מזוהים חייבות להיות מוגבלות לזיהוי המטרה בלבד. מרגע שזוהתה כמטרה זרה יש להשמיש מסגרות משפטיות לפעילות אכיפת חוק חוצת-גבולות, ולהקפיד על יידוע המדינה הרלוונטית

---

to effectuate remote searches, and whose property may be targeted. Moreover, although the ex ante warrant process regulates some aspects of network investigative techniques, it does so without regard to national security or international norms. A warrant may impose constitutional limitations that check the intensity and breadth of hacking techniques. But cross-border cyberoperations will still be unilateral, invasive, and conducted without coordination with the agencies that lead U.S. foreign relations and national security policy").

ראו מנגד את עמדתם ההפוכה של קר ומרפי לעניין זה: Orin S. Kerr & Sean D. Murphy, *Government Hacking to Light the Dark Web*: *What Risks to International Relations and International Law?*, 70 STANFORD L. REV. ONLINE 58 (2017).

[118] יודגש כי חלק מההמלצות שמעלה גאפור נדחו מפורשות במשרד המשפטים האמריקאי בשלב גיבוש התיקון לסעיף 41 וראו: Memorandum from David Bitkower, Assistant Attorney Gen., Criminal Div., to the Honorable Reena Raggi, Chair of the Advisory Committee on Criminal Investigations (Oct. 20, 2014) (Response to Post on Proposed Amendment to Rule 41) (להלן: https://www.uscourts.gov/sites/default/files/fr_import/CR2015-05.pdf) מכתב מטעם סגן התובע הכללי לעניין התיקון לסעיף 41).

[119] גאפור, לעיל ה"ש 115, בעמ' 1124–1128.

[120] שם, בעמ' 1128–1129 (בטענה כי יש לצמצם את השימוש בכלי התקיפה רק למטרות איתור מיקומו של היעד ולא לביצוע פעולות אחרות האפשריות באמצעות הכלי) ושוב בעמ' 1134 (בקביעה כי על הקונגרס לקבוע גבולות לרכש טכנולוגיות תקיפה, כדי שיימנע רכש של טכנולוגיות שאינן עולות בקנה אחד עם סטנדרטים שנקבעו כחלק מ"פרוצדורת נכסי החולשה". ראו דיון בפרוצדורה זו בעמודים הבאים). עמדה זו של גאפור נדחתה מפורשות בידי סגן התובע הכללי בטענה שאין להגביל את שיקול הדעת של הרשות המבצעת לבחור באמצעים, וכי בחירות אלה צריכות להתבצע מתוך שיקולים עניינים ובהתחשב בנסיבות. ראו שם, בעמ' 3.

ומימוש הסדרים דיפלומטיים, אם אלה זמינים, ובייחוד אמנות לעזרה משפטית הדדית בעניינים פליליים (Mutual Legal Assistance Treaties, או MLAT).[121]

שלישית, כדי להימנע מאבחון חיובי שגוי (false positives) יש להבטיח שכל תקיפה בנפרד נעשית נגד יעד שיש יסוד סביר להניח כי הוא מוחזק בידי חשוד בעבירה פלילית או עבריין נמלט, או כי באמצעות האמצעי הדיגיטלי המותקף מבוצעות עבירות על הדין האמריקאי (לפי דרישת "היסוד הסביר" (ה-Probable Cause) המעוגנת בתיקון הרביעי לחוקה האמריקאית).[122] כמו כן הציע גאפור כי יאומץ עקרון הנחיצות שמכוחו לא תאושר פעולת פצחנות בטרם תיבחנה אפשרויות חקירתיות חלופיות שפגיעתן בזכות לפרטיות פחותה.[123]

רביעית, אף שמשרד המשפטים קבע כי הוא רשאי להשמיש פעולות פצחנות מסוג אלה נגד כל עבירה, מציע גאפור כי נכון לצמצם את השימוש בכלי זה רק בהקשרן של עבירות חמורות (דוגמת עבירות טרור), או שיש בעניינן קונצנזוס בין-לאומי (דוגמת פורנוגרפיית ילדים או עבירות סחר בסמים).[124]

---

[121] שם, בעמ' 1128–1129. לדיון על המגבלות שפעילות בענן מייצרת על שימוש במנגנוני MLAT ראו: Jennifer C. Daskal, *Borders and Bits*, 71 VANDERBILT L. REV. 179 (2018).

[122] שם, בעמ' 1129. בהקשר הזה הדין האמריקאי מאפשר כיום הוצאת צווים מקדמיים (Anticipatory Warrants). דרישת ההקפדה (Particularity) המעוגנת בתיקון הרביעי לחוקה האמריקאית מאפשרת לשוטרים לתאר מראש תניות שבהתקיימן תקום לרשות המבצעת הסמכות להפעיל פעולת פצחנות. ראו: Jonathan Mayer, *Constitutional Malware*, Stanford University School of Engineering Paper Series (Nov. 14, 2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2633247 ("Agents may not know, in advance, the exact computer that they are breaching. But they can articulate a conditional set of facts to ensure a fair chance that their malware will be delivered, and when it is delivered, to a computer system that satisfies probable cause and particularity"). כך למשל בהקשר של פרשת Playpen אחת התניות יכולה להיות תקיפה של כל מי שמשתמש באתר פורנוגרפיית הילדים, שכן השימוש בפני עצמו עולה לכדי עבירה על הדין האמריקאי.

[123] גם עמדה זו נדחתה בידי סגן התובע הכללי בטענה שיהיה שגוי להסמיך את הרשות השופטת להתערב בתהליכי קבלת החלטות שיש להם גם נפקות מבצעית-חקירתית וגם נפקות במישורי יחסי החוץ. ראו מכתב מטעם סגן התובע הכללי לעניין התיקון לסעיף 41, לעיל ה"ש 118, בעמ' 3.

[124] גאפור, לעיל ה"ש 115, בעמ' 1129–1131.

לבסוף קובע גאפור כי יש להגדיל את הביקורת הפרלמנטרית של הקונגרס על פעילויות פצחנות המבוצעות מכוח סעיף 41, בין היתר באמצעות יצירת חובות דיווח תקופתיות וישירות לקונגרס של ה-FBI.[125]

על אלה ראוי להוסיף כי לשון התיקון לסעיף 41 משאירה עמומה את שאלת השימוש בנוזקה למטרות פעילות אקטיבית ולא פסיבית על המכשיר (דוגמת הפעלת מיקרופון או מצלמה או שינוי במידע). יש להעריך כי פעולות מסוג אלה יסווגו כהאזנה בזמן אמת, ולכן יחייבו עמידה בדרישות המחמירות להוצאת צווים של חוק האזנת סתר האמריקאי (The Wiretap Act).[126] זאת גם עמדת משרד המשפטים האמריקאי.[127]

ככלל, הדין האמריקאי מציב חובות שלאחר מעשה (*ex post*) על הרשויות שביצעו פעולת פצחנות. כך לדוגמה הדין מחייב חובת דיווח על התקיפה הגם שחובה זו יכול שתתמלא, לפי צורכי הפעילות, גם לאחר שפעולת הפצחנות הסתיימה (ולא בהכרח בהגשת עותק מהצו לגורם הנחקר במועד התקיפה, כמקובל בפעולות חיפוש סטנדרטיות). עוד חלות דרישות תיעוד של פעולת הפצחנות ושל המידע שנאסף ממנה. הפרטים שנמסרים לשופט המאשר יכול שיוגבלו למידע שנאסף מבלי לציין את מתודת ההתפשטות או את אופן פעילות הנוזקה.[128]

<u>3.א.4. המסגרת החוקית לפעילות פצחנות מודיעינית מצד יחידות הביון</u>

ראוי להתייחס בקצרה לשתי נקודות נוספות הנוגעות לפעולות פצחנות בדין האמריקאי. ראשית, ידוע זה מכבר כי גופי ביון אמריקאיים, ובייחוד ה-CIA וה-

---

[125] שם, בעמ' 1132–1135.

[126] בספרות נוהגים לרוב להתייחס לדרישות המחמירות של חוק האזנת סתר האמריקאי כדרישת ה- Super Warrant. לקריאה נוספת על חוק האזנת סתר האמריקאי ראו: פוקס, לעיל ה"ש 68, בעמ' 270–271. לקריאה על אפשרות החלת הדרישות המחמירות של החוק בהקשר של פעולות פצחנות ראו: מחקר הפרלמנט האירופי, לעיל ה"ש 108, בעמ' 124–125. יודגש כי משרד המשפטים האמריקאי שקל את הרעיון של החלת דרישת ה-Super Warrant על פעולות פצחנות ודחה אותו.

[127] ראו: מכתב מטעם סגן התובע הכללי לעניין התיקון לסעיף 41, לעיל ה"ש 118, בעמ' 9.

[128] ראו: שם, בעמ' 7–9. עוד ראו: מחקר הפרלמנט האירופי, לעיל ה"ש 108, בעמ' 124.

NSA, עושים שימוש נרחב בפעולות פצחנות למימוש המנדט שלהם לאיסוף מודיעין זר.[129] ההסדרה המשפטית של הסמכות של גופים אלה לביצוע התקיפות לוטה בערפל. ההערכה המקובלת היא כי הבסיס המשפטי מצוי בצו נשיאותי 12333 שנחתם ב-4 בדצמבר 1981 בתקופת ממשל רייגן. הצו, שכותרתו "פעילויות המודיעין של ארצות הברית" קובע את תחומי האחריות של סוכנויות הביון של ארצות הברית, לרבות את סמכותן בביצוע פעילויות מודיעין שאינן מוסדרות מכוח דבר חקיקה אחר.[130]

לבסוף יודגש כי ארצות הברית היא המדינה הראשונה בעולם שהודתה במוצהר כי היא אוגרת חולשות אפס ימים, והיא גם המדינה היחידה אפוא שפיתחה מנגנון לפיקוח על תהליך הדיווח על חולשות אלה ליצרניות. המנגנון המכונה "פרוצדורת נכסי חולשה" (Vulnerabilities Equities Process או VEP) גובש בימי ממשל אובמה, ומכוחו קמה ה-Equities Review Board כפורום המרכזי לדיון ובחינה באגירה ובפרסום של חולשות מצד גורמי הביטחון בארצות הברית. המנגנון קובע אילו סוכנויות רשאיות לשלוח נציגים לוועד, מהו המנדט של הוועד, אילו שיקולים צריכים להנחות את הוועד בתהליך קבלת ההחלטות שלו, מהן פרוצדורות

---

[129] ראו לדוגמה: Keith Collins, *Wikileaks: The CIA can remotely hack into computers that aren't even connected to the internet*, QUARTZ (Jun. 24, 2017), https://qz.com/1013361/wikileaks-the-cia-can-remotely-hack-into-computers-that-arent-even-connected-to-the-internet/; Reuters, *What Do I Need to Know About the CIA's Hacking Program?*, FORTUNE (Mar. 7, 2017), https://fortune.com/2017/03/07/cia-hacking-explained; Ken Dilanian, *Can the CIA and NSA Be Trusted with Cyber Hacking Tools*, NBC NEWS (Jun. 30, 2017) https://www.nbcnews.com/news/us-news/can-cia-nsa-be-trusted-cyber-hacking-tools-n778731; Ryan Gallagher & Glenn Greenwald, *How the NSA Plans to Infect 'Millions' of Computers with Malware*, THE INTERCEPT (Mar. 12, 2014) https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/. עוד יובהר כי למעשה גם ה-FBI מעורב בפעולות פצחנות חוצות-גבולות, וראו: מכתב מטעם סגן התובע הכללי לעניין התיקון לסעיף 41, לעיל ה"ש 118, בעמ' 2 (שם מבהיר סגן התובע הכללי, בתגובה לגאפור, כי מנקודת המבט של ה-FBI, היות שהתיקון הרביעי לחוקה האמריקאית לא חל חוץ-טריטוריאלית, אין כל מניעה משפטית מהסוכנות לבצע פעולות חיפוש שכאלה).

[130] לקריאה נוספת על הצו הנשיאותי 12333, לרבות בהקשר של פעולות פצחנות, ראו: Mark Jaycox, *A Primer on Executive Order 12333: The Mass Surveillance Startlet*, EFF (Jun. 2, 2014), https://www.eff.org/deeplinks/2014/06/primer-executive-order-12333-mass-surveillance-starlet.

העבודה של הוועד, ומהן חובות הדיווח שלו.[131] ה-PATCH Act, הצעת חוק המבקשת לעגן בחקיקה ראשית את המנגנון, תלויה ועומדת בקונגרס.[132]

3.ב. הדין האנגלי

3.ב.1. המסגרת החוקית לפעילות פצחנות מודיעינית מצד יחידות ביון וגופי שיטור

ב-29 בנובמבר 2016 קיבל "חוק כוחות החקירה" הבריטי (ה- Investigatory Powers Act, או IPA) את הגושפנקה המלכותית והפך לחוק. החוק אורכו 291 עמודים, והוא מלווה בעוד שישה "קודי התנהגות" (Codes of Practice) שגיבש משרד הפנים הבריטי, שאורכם הכולל הוא יותר מ-1,000 עמודים. החוק מעגן את עיקרי סמכויות החקירה של גופי הביון ואכיפת החוק בממלכה המאוחדת.[133] חלקים 5 ו-6 (פרק 3) לחוק, שעניינם Equipment Interference (EI), מעגנים את עיקר הסמכות לביצוע פעולות פצחנות בדין האנגלי.[134] קוד ההתנהגות מונה כדוגמאות לפעילות EI הורדה

---

[131] לקריאה נוספת על המנגנון, ראו: Vulnerabilities Equities Policy and Process for the United States Government, WHITE HOUSE (Nov. 15, 2017), https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF; ראו נספח 3: מנגנון העבודה של תהליך VEP והשיקולים המנחים את הוועד.

[132] ראו: Protecting Our Ability to Counter Hacking Act of 2017, H.R. 2481, 115th Cong. (2017); לדיון ביקורתי על הצעת החוק ראו: Mailyn Fidler & Trey Herr, *PATCH: Debating Codification of the VEP*, LAWFARE (May. 17, 2017), https://www.lawfareblog.com/patch-debating-codification-vep.

[133] ראו: Investigatory Powers Act 2016, c.25. §5, §6 (Chapter 3) (Eng.).; לקריאה נוספת ראו: Asaf Lubin, *The Investigatory Powers Act and International Law: Part I*, UCL JOURNAL OF LAW AND JURISPRUDENCE BLOG (Dec. 26, 2016) https://blogs.ucl.ac.uk/law-journal/2016/12/26/the-investigatory-powers-act-and-international-law-part-i/.

[134] יובהר כי פעולות חיפוש בחומר מחשב שלא על דרך של פעולת פצחנות, לדוגמה חדירה לחומר מחשב בהסכמת המשתמש, איננה מחייבת הוצאת צו EI על פי הדין האנגלי. הדין

חשאית של מידע ממחשב נייד או מטלפון חכם באמצעות התקנת תוכנת רוגלה במכשיר; התקנת "רשם הקשות" במכשיר כדי לאסוף מידע על פרטי המשתמש בעת כניסתו לאתר אינטרנט כלשהו.[135]

לעומת צווי EI, המאשרים איסוף של כל החומר השמור במערכת, כל איסוף של חומר בזמן אמת מחייב הוצאת צו האזנת סתר נוסף (כמעוגן בחלק 2 ובחלק 6 (פרק 1) לחוק).[136] פעילות אקטיבית לביצוע מעקב על סביבתו של המשתמש, לרבות בביתו וברכבו של המשתמש (באמצעות הפעלה מרחוק של מצלמה, מיקרופון או אפליקציות נוספות) מאושרים מכוח צו EI, אך על הבקשה לפרט את כל הפעולות המתוכננות.[137] כחלק מהבקשה לצו יש לכלול כל מידע על פעילות אגבית צפויה אשר

האנגלי מגדיר את המונח EI כך: "Equipment interference describes a range of techniques used by the equipment interference authorities that may be used to obtain communications, equipment data or other information from equipment. Equipment interference can be carried out either remotely or by physically interacting with the equipment. Equipment interference operations vary in complexity. At the lower end of the complexity scale, an equipment interference authority may covertly download data from a subject's mobile device when it is left unattended, or an equipment interference authority may use someone's login credentials to gain access to data held on a computer. More complex equipment interference operations may involve exploiting existing vulnerabilities in software in order to gain control of devices or networks to remotely extract material or monitor the user of the device" וראו: Home Office, *Equipment Interference Draft Code of Practice*, 9 (Dec. 2017), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/668940/Draft_code_-_Equipment_Interference.pdf (להלן: קוד התנהגות בפעולות פצחנות).

[135] שם. לקריאה נוספת ראו: כהנא ושני, לעיל ה"ש 68, בעמ' 168–171.

[136] שם, בעמ' 11. לדוגמה איסוף שיחת וידאו אונליין שמבצע המשתמש עם משתמש אחר. לתיאור תהליך הגשת כמה צווים בעת ובעונה אחת, ראו שם, בעמ' 59–61.

[137] שם, בעמ' 12. יש להבחין בין פעילות מעקב (surveillance) לבין פעולות אקטיביות למניפולציה או מחיקה של מידע במכשיר או במערכת, המוגדרות בדין האנגלי Property Interference. כך למשל פעולה לשיבוש פעילותה של מצלמת אבטחה או הפסקתה, גם אם כחלק ממנה אוספת הרשות החוקרת את כל הצילומים מהמצלמה, אינה יכולה להיות מאושרת מכוח צו EI. פעולה כזאת יכולה לחייב אישור נפרד מכוח חלקים 5 או 7 ל-Intelligence Services Act, 1994 או חלק 3 ל-Police Act, 1997. ראו שם, בעמ' 19.

תידרש לשם השלמת החדירה למערכת. עם זאת החוק מבהיר כי במקרים לא צפויים, אגב ביצוע פעולת החדירה והאיסוף, שמורה לסוכנות המבצעת מרחב שיקול דעת.[138]

ככלל מבחין החוק בין שלושה סוגי צווים: צו ממוקד להפרעה למכשיר (Targeted EI Warrant), צו בחינה ממוקד (Targeted Examination Warrant) וצו נפח להפרעה למכשירים (Bulk EI Warrant). גופי הביון רשאים להגיש בקשה לשלושת סוגי הצווים, ואילו רשויות אכיפת חוק ושיטור מוגבלות לצווים מן הסוג הראשון.[139] בדומה לזה, צווי נפח אפשריים רק לטובת השגת מודיעין זר או נגד מטרות זרות, ואילו צווים ממוקדים נועדו לשימוש כחלק מפעולות פצחנות בשטחי האיים הבריטיים. יובהר כי למרות השם המתעתע, צווים ממוקדים להפרעה למכשירים אינם חייבים להיות ממוקדים למכשיר אחד בלבד. בפועל החוק מאפשר הוצאה של "צווים תמטיים" (Thematic Warrants), דהיינו צו לאיסוף מידע או נתונים מכמה מכשירים בעלי מאפיינים משותפים, או שלמשתמשיהם מאפיינים משותפים.[140] ביקורת רבה הוטחה מצד ארגוני חברה אזרחית על הסמכות הזאת ועל החשש שמא החוק מאפשר בפועל הוצאה של צווי נפח בשם אחר.[141]

---

[138] כך למשל מדגים הקוד כי גם אם אושרה בצו החדירה לכונן ספציפי ובזמן אמת, ובמהלך המבצע מזהים החוקרים שני כוננים, ואין ביכולתם לזהות מי מהם הוא הכונן שחדירה אליו אושרה, רשאים הם לאסוף מידע על שני הכוננים עד לזיהוי הכונן הרלוונטי. כל מידע שנאסף על הכונן הנוסף יימחק בהקדם האפשרי. שם, בעמ' 12.

[139] לרשימה המלאה של הגופים המוסמכים להוציא צווי EI ראו שם, בעמ' 21 (ככלל הרשימה כוללת קציני משטרה, קציני הגירה, קציני מכס, ונציגי הרשות להגבלים עסקיים). יובהר כי גופי ביון בריטיים העוסקים במודיעין פנים (דוגמת ה-MI5 וה-NCA) מוסמכים להוציא צווים מכל הסוגים. באשר לצווי בחינה, אלה מחוץ לגבולות נייר זה. מטרתם לאפשר בחינה מוגבלת של מידע שנאסף באמצעות צווי נפח, ואשר עשוי לכלול גורמים המצויים בתוך האיים הבריטיים. לדוגמה: זר שהושמש נגדו צו נפח מגיע לגבולות האיים הבריטיים. הוצאת צו בחינה תאפשר את המשך המעקב אחר אותו זר עד למועד שבו הבקשה לצו ממוקד תאושר.

[140] לקריאה נוספת על השימוש בצווים תמטיים ראו, שם, בעמ' 30–33. אחת הדוגמאות המובאות בקוד היא שימוש במתקפת "באר המים" על אתר אינטרנט שמשמש להשגת מידע למטרות תכנון וביצוע פעולות טרור. תיאור כללי של האתר ושל הצורך בזיהוי היעדים הנכנסים אליו הוא מספק למטרות הוצאת "צו תמטי". ניכר אפוא כי שימוש בצווים כאלה יהיה רלוונטי במיוחד בהקשר של תקיפות נגד יעדים לא מזוהים (וראו הדיון בדבר אנונימיות ברשת האפלה לעיל).

[141] ראו לדוגמה: Gus Hosein, *The UK Investigatory Powers Act: A Bad Example for the World*, PRIVACY INTERNATIONAL (Jan. 17, 2017) https://medium.com/privacy-international/the-uk-investigatory-powers-act-a-bad-example-for-the-world-4e51b0d126b0.

2.ב.3. איזונים ובלמים הקבועים בחוק

בהגשת הבקשה לצו ובתהליך אישורו מונה החוק כמה וכמה עקרונות מנחים לבחינה: ראשית עקרון הנחיצות קובע כי על פעולת פצחנות לשרת אחת משלוש מטרות: הגנה על ביטחון המדינה, זיהוי או מניעה של פשע חמור[142] או הגנת החוסן הכלכלי של הממלכה המאוחדת (כשאינטרסים אלה רלוונטיים לאינטרסים של ביטחון לאומי). דרישת הנחיצות למעשה מעגנת את מבחן הקשר הרציונלי המוכר מדיני החוקה הישראליים.[143]

שנית, מכוח עקרון המידתיות מעוגן מבחן הפגיעה הפחותה ומבחן המידתיות במובן הצר (מאזן אינטרסים). החוק מונה כמה שיקולים מנחים: (א) האינטרס הציבורי בשמירה על ביטחון מערכי תקשורת (לרבות רשת האינטרנט בכללותה) ושלמותם; (ב) האינטרס הציבורי בהגנה על הזכות לפרטיות והיקף ההפרעה לזכות; (ג) האינטרס של משתמשים אחרים בציוד או במערכות המותקפות; (ד) אם המידע המבוקש רגיש באופן מיוחד, המצדיק הטיה של המאזן.[144] דגש מיוחד מושם בקוד

---

[142] פשע חמור מוגדר כעבירה שעונשה הוא יותר משלוש שנות מאסר, או שהיא כרוכה באלימות, בהשגת רווח כלכלי ניכר או בהתארגנות של מספר רב של אנשים בעלי מטרה משותפת.

[143] קוד התנהגות בפעולות פצחנות, לעיל ה"ש 134, בעמ' 22–23, 26. כפי שהקוד מבהיר: "Equipment interference authorities must not intrude into privacy any more than is necessary to carry out their functions or enable others to do so. To leave targets open to exploitation by others would increase the risk that their privacy would be unnecessarily intruded upon. Equipment interference activity must therefore be carried out in such a way as to appropriately minimise the risk of any increase in the likelihood or severity of any unauthorised intrusion into the privacy; or increase in the risk to the security, of users of equipment or systems (whether or not those equipment or systems are subject to the activities of the equipment interference authority)".

[144] שם, בעמ' 25–27. בהקשר הזה הקוד מבהיר כי בבקשה לצו יש לכלול כל סיכון לביטחון או לשלמות מערכות ורשתות וכל הצעדים המתוכננים כדי להקטין את הסיכוי לנזק. דגש מיוחד מושם בקוד בבחינה מוגברת של מידתיות בהקשר של תקיפת תשתיות לאומיות.

לצמצום הסיכון לאיסוף של "מידע אגבי" כחלק מפעולת הפצחנות (מה שמכונה Collateral Intrusion).[145]

שלישית, מכוח עקרון אמצעי הביטחון מונה הקוד כמה כללים שיש ליישמם בכל העתקה, אגירה ומסירה של מידע שנאסף בפעולת פצחנות. על הרשות החוקרת לתאר כיצד תיישם אמצעים אלה בתהליך הגשת הבקשה, ועל הרשות המאשרת לבחון אם דרישת אמצעי הביטחון מסופקת דייה.[146] דגש מיוחד מושם בקוד על גיבוש אמצעי ביטחון בהקשר של שיתופי פעולה מודיעיניים בין-משרדיים ועם גורמי חוץ.[147]

לבסוף, החוק מונה הגנות מיוחדות ושינויים בפרוצדורה בכל האמור באיסוף מידע שכפוף לחיסיון עיתונאי, לחיסיון משפטי (חסיון עורך דין–לקוח לדוגמה), לחיסיון רפואי או לחיסיון פרלמנטרי.[148]

הפרוצדורה לאישור בקשות לצו לפי ה-IPA, לרבות בהקשר של צווי EI, מכונה בדין האנגלי גישת "המנעול הכפול" (ה-double lock). הבקשה צריכה להיות מאושרת פעם אחת בידי שר החוץ (לבקשת ראש שירות המודיעין הרלוונטי) או ראש רשות האכיפה הרלוונטית (לבקשת נושא משרה באותה רשות לאכיפת חוק) ופעם שנייה בידי הנציב המשפטי (Judicial Commissioner). בשני המקרים תיבדק הבקשה לצו בראי העקרונות המנחים המנויים לעיל.[149] הנציב המשפטי רשאי לדרוש מידע נוסף, לסרב לאשר את הצו בתוספת נימוקים או להעביר את הבקשה לעיונו של נציב כוחות החקירה (Investigatory Powers Commissioner, או IPC).[150] החוק קובע גם

---

[145] שם, בעמ' 48–49. כך הקוד מביא כדוגמה צורך באחסון מידע על מיקומו של א דרך ביצוע פעולת פצחנות על שותפו הלא מעורב – ב. הקוד קובע כי כל איסוף מידע על ב וסביבתו, לרבות כל אלה שעימם הוא בא בקשר, יישקלו כ"מידע אגבי" שיש להביאו בחשבון בטרם אישור הפעולה.

[146] שם, בעמ' 106–136. זאת לרבות כללים בדבר מחיקה וביעור של חומר שנאסף, הכללים בדבר הגישה לחומר שנאסף והשימוש בו כראיה בהליכים משפטיים, הכללים בדבר מסירת חומר שנאסף לגורמים שלישיים, חובות דיווח על טעויות לאורך התהליך לרבות לנציב המשפטי.

[147] שם, בעמ' 114.

[148] שם, בעמ' 115–121.

[149] שם, בעמ' 28, 49. לרשימה המלאה של כל המרכיבים של הבקשה לצו ראו עמ' 37–39. למרכיביו של הצו לאחר אישורו ראו עמ' 42–43.

[150] שם, בעמ' 50. אם גם נציב כוחות החקירה דוחה את הבקשה, הצו לא יאושר, ללא אפשרות לערעור נוסף.

מסגרת לאישור צווים דחופים,[151] להארכתם[152] או לשינוים.[153] החוק האנגלי מאפשר לדרוש "סיוע סביר" מכל אדם במימוש צווי EI, אך הוא מטיל חובת עשה על ספקיות תקשורת וקובע את המנגנון שדרכו תוגש הבקשה לסיוע, לרבות היכולת להטיל קנסות על אי-מילוי החובה בהקשרים מסוימים.[154]

עיקר הביקורת השיפוטית מעוגנת בתפקידם של הנציבים המשפטיים ונציב כוחות החקירה. נציב כוחות החקירה הראשון לורד אדריאן פולפורד, אשר נבחר במרס 2017 בידי ראש הממשלה למינוי בן שלוש שנים, משקף את מידת העצמאות והרקע המשפטי המצופה מהמחזיק בתפקיד.[155] נוסף על זה רשאי כל אדם להגיש תלונה או מחלוקת בדבר שימוש בכלי האזנה לפי ה-IPA לטריבונל מיוחד ה-IPT.[156] הן הטריבונל והן נציב כוחות החקירה רשאים להיוועץ במומחי טכנולוגיה.[157]

<u>3.ב.3. המסגרת החוקית לפעילות פצחנות למטרות איסוף מודיעין חוץ</u>

---

[151] במקרה שבו לא ניתן להשיג את אישור הנציב המשפטי בזמן שיאפשר את הגשמת המטרות האופרציונליות של הפעילות (בדגש על סיכון לחיים או לנזק חמור או חלון הזדמנויות מודיעיני מוגבל) יאשר את הבקשה בעל התפקיד הרלוונטי, ותועבר לבחינתו של הנציב המשפטי בתוך שלושה ימים. צווים רגילים תוקפם חצי שנה, ואילו צווים דחופים טרם חידושם טובים לחמישה ימים בלבד. אם הנציב המשפטי דוחה בקשה שאושרה בהליך חירום, על הרשות להפסיק פעולת הפצחנות מייד, בגבולות הסביר. ראו שם, בעמ' 50–51.

[152] שם, בעמ' 51–52.

[153] שם, בעמ' 52–57.

[154] שם, בעמ' 85–90. לצד זאת מעגן החוק מנגנון של Technical Capability Notice כמנגנון נוסף שדרכו ניתן לדרוש סיוע טכנולוגי מספקיות תקשורת כחלק מההסדרה ב-IPA.

[155] לקריאה נוספת על המינוי ראו: Alexander J. Martin, *UK's First Investigatory Powers Commissioner: Lord Justice Fulford*, THE REGISTER (Mar. 3, 2017) https://www.theregister.co.uk/2017/03/03/uks_first_investigatory_powers_commissioner_lord_justice_fulford. בטרם מינויו לתפקיד היה לורד פולפורד שופט בבית הדין הבין-לאומי הפלילי בהאג (2003-2012) וכן חבר במועצה הלאומית לזכויות אזרחיות.

[156] לקריאה נוספת על הטריבונל ראו כהנא ושני, לעיל ה"ש 68, בעמ' 178–180 (מדובר במותב עצמאי המורכב משופטים בכירים, פעילים או בדימוס, וממשפטנים בכירים, הממונים לתקופה בת חמש שנים. הטריבונל רשאי לקבוע פיצויים למתלוננים).

[157] לקריאה נוספת ראו: מחקר הפרלמנט האירופי, לעיל ה"ש 108, בעמ' 107.

באשר לפעולות פצחנות שמבצעים גופי הביון הבריטיים מחוץ לגבולות האיים הבריטיים ה-IPA אינו מקים חובה בשימוש בצווי EI. אותם גופי ביון מוסמכים לפעול גם מכוח הסמכות הכללית השמורה להם לפי חלק 7 ל- Intelligence Services Act, 1994. עם זאת הקוד מבהיר כי יש מקרים שבהם הוצאת צו EI תהיה רצויה, גם אם לא מחויבת, לדוגמה בכל האמור בשטחים המצויים בשליטה אפקטיבית של בריטניה (שגרירויות, בסיסים צבאיים ומתקני מאסר), אשר בהקשרם אפשר שיקומו חובות מכוח אמנות זכויות אדם שבריטניה היא צד להן.[158]

יש מעט מאוד מידע זמין באשר לכלים הטכנולוגיים שבהם בריטניה משתמשת כחלק מפעולות פצחנות, ובייחוד באשר לסוגי הנוזקות או אופן האגירה של חולשות. ניסיונות להגיש בקשת חופש מידע על שיטות אלה לא צלחו בעבר.[159] עם זאת לאחרונה חשפה אנגלייה כי גם לה יש מנגנון "פרוצדורת נכסי חולשה" (VEP). את המנגנון מנהלת סוכנות מודיעין האותות של המדינה, ה-GCHQ. המודל דומה במרכיביו למקבילה האמריקאית.[160]

3.ג. הדין הצרפתי

3.ג.1. רקע היסטורי

שנת 2015 זכורה כשנה קשה בתודעה הצרפתית, שנה שראשיתה בינואר במתקפה על שארלי הבדו וסופה בנובמבר בפיגועי הטרור בפריז.[161] על רקע התקיפות האלה אישר

---

[158] שם, בעמ' 18.

[159] ראו: מחקר הפרלמנט האירופי, לעיל ה"ש 108, בעמ' 108. עוד ראו: Joseph Cox, *UK Police Are Using Hacking Tools But Refuse to Say How*, MOTHERBOARD (Dec. 23, 2015), https://www.vice.com/en_us/article/d7y89z/uk-police-are-using-hacking-tools-but-refuse-to-say-how.

[160] לקריאה נוספת ראו: *The Equities Process*, GCHQ (Nov. 29, 2018), https://www.gchq.gov.uk/information/equities-process (להלן: פרוצדורת נכסי חולשה – אנגלייה).

[161] ראו: פרדי איתן "מדוע סומנה צרפת כמטרה מועדפת לטרור והאם תצליח במלחמתה?" **המרכז הירושלמי לענייני ציבור ומדינה** 15.11.2015 goo.gl/mkMuYk.

הפרלמנט הצרפתי שני חוקים שהרחיבו את סמכויות הריגול והמעקב של סוכנויות הביון ואכיפת החוק הצרפתיים: הראשון, "חוק המודיעין", שהתקבל ב-24 ביולי 2015,[162] והשני "החוק לחיזוק המאבק בפשיעה המאורגנת, בטרור, ובאמצעי המימון שלהם", שהתקבל ב-3 ביוני 2016.[163] אין זה מפתיע כי שני החוקים עיגנו סמכויות לביצוע פעולות פצחנות מצד הרשויות.

3.ג.2. המסגרת החוקית לפעילות פצחנות מודיעינית מצד יחידות הביון

מכוח החוק הראשון שונה הקוד לביטחון פנים כך שהוכרה סמכותם של גופי המודיעין הצרפתיים להשמיש אמצעים טכניים כדי (1) להשיג גישה למידע השמור במערכת מחשב, לאסוף אותו ולהעבירו; או (2) להשיג גישה למידע שמוצג על צג מחשבו של משתמש (לרבות מידע שהוקש ומידע שנאסף באמצעות עזרים אודיו-ויזואליים פריפריאליים דוגמת מיקרופונים, מצלמות וסנסורים), לאסוף אותו ולהעבירו.[164] פעולות פצחנות מן הסוג הראשון מאושרות לתקופה של 30 ימים. פעולות

---

[162] ראו: Loi 2015-912 du 24 juillet 2015 relative au renseignement [Law 2015-912 of July 24, 2015 relating to Intelligence], JOURNAL OFFICEL DE LA REPUBLIQUE FRACAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], Jul. 26, 2015, p. 12735. (להלן: חוק המודיעין).

[163] ראו: Loi 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale [Law 2016-731 of June 3, 2016 reinforcing the fight against organized crime, terrorism, and their financing, and improving the efficiency and guarantees of criminal procedural], JOURNAL OFFICEL DE LA REPUBLIQUE FRACAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], Jun. 4, 2016. (להלן: החוק לחיזוק המאבק בפשיעה המאורגנת, בטרור ובאמצעי המימון שלהם).

[164] ראו: חוק המודיעין, לעיל ה"ש 162, בסע' L.853-2. יובהר כי סמכויות אלה נוגעות לפעולות פצחנות של גופי המודיעין הצרפתיים בתוך גבולות צרפת. ב-30 בנובמבר 2015 אישר הפרלמנט הצרפתי את חוק המודיעין הזר, שעניינו איסוף מודיעין מחוץ לגבולות צרפת. בניגוד לחוק הראשון, חוק זה לא הזכיר כלל פעולות פצחנות. לפיכך אין הסדרה מפורשת בחקיקה ראשית בדין הצרפתי לפעולות פצחנות חוצות-גבולות. ראו: Loi 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications electroniques internationales [Law 2015-1556 of November 30, 2015 relating to Surveillance

פצחנות מן הסוג השני מאושרות לתקופה של עד חודשיים. ניתן לאשר מחדש כל אחת מהפעולות שוב, באותם קבועי זמן, ללא מגבלה על מספר האישורים החוזרים.[165] המידע שנאסף כחלק מפעולות אלה יכול להישמר לתקופה של עד 120 ימים, הנתונה גם היא לאישור חוזר.[166] החוק מונה הסדר מיוחד בשימוש בפעולת פצחנות למטרות מעקב אחר ביתו או רכבו של אדם.[167] עוד מונה החוק הגנות מיוחדות במקרה שהמידע כפוף לחסינות כדין (חברי פרלמנט, שופטים, עורכי דין או עיתונאים).[168]

פעולות פצחנות אלה יכול שיאושרו כדי להגן על האינטרסים החיוניים לצרפת ולקדמם, לרבות אלה: (א) עצמאותה הלאומית, שלמותה הטריטוריאלית וביטחונה הלאומי; (ב) צורכי מדיניות החוץ של צרפת, ביצוע החובות האירופיות והבין-לאומיות של צרפת ומניעת כל התערבות זרה בענייניה הפנימיים; (ג) האינטרסים הכלכליים, התעשייתיים והמדעיים החיוניים של צרפת; (ד) מניעת טרור; (ה) סיכול תקיפות נגד הרפובליקה ומוסדותיה, לרבות אלימות קולקטיבית אשר בחומרתה מפריעה לשלום הציבורי; (ו) מניעת פשיעה מאורגנת ועבריינות חמורה; (ז) מניעת פרוליפרציה של נשק להשמדה המונית.[169]

3.ג.3. איזונים ובלמים הקבועים בחוק

הסמכות לאשר פעולות פצחנות אלה נתונה לראש הממשלה לבקשת אחד השרים האלה: הביטחון, הפנים או האוצר.[170] ראש הממשלה מחויב בהיוועצות עם גוף מפקח, "המועצה הלאומית לבקרה על טכניקות מודיעין" (CNCTR), שבה תשעה חברים (ארבעה נציגי פרלמנט המבטאים ייצוג פלורליסטי של הדעות בבית המחוקקים; שני נציגים של מועצת המדינה של צרפת; שני שופטים; מומחה טכנולוגי

Measures of International Electronic Communications], JOURNAL OFFICEL DE LA REPUBLIQUE FRACAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], Dec. 1, 2015, p. 22185.

[165] שם.

[166] שם, בסע' L.822-2.

[167] שם, בסע' L.853-3.

[168] שם, בסע' L.821-7.

[169] שם, בסע' L.811-3.

[170] שם, בסע' L.811-4.

הממונה בהמלצת הרשות הלאומית לתקשורת אלקטרונית ודואר).[171] במקרים דחופים רשאי ראש הממשלה לאשר פעולת פצחנות גם מבלי להיוועץ ב-CNCTR ובתנאי שיעדכן את המועצה בתוך 24 ממועד אישור הבקשה, לרבות הנסיבות שהצדיקו את הדחיפות.[172] יתרה, מזאת המועצה מוסמכת לקבוע הסדרים נוספים בכל האמור בכלים ובטכניקות שאותם משמישים גופי המודיעין כחלק מפעולת הפצחנות.

בבואה לבחון בקשות לפעולות פצחנות או אמצעים טכנולוגיים ספציפיים, על המועצה לשקול את האינטרסים הקבועים בזכות לפרטיות ובזכות להגנת מידע פרטי. כמו כן עליה לאשר כי הפעולה מבוצעת כחוק לפי הסמכות שמסורה לרשות החוקרת, נחוצה לאחת מהמטרות שתוארו לעיל, ומוצדקת בשל האיומים והסיכונים לאינטרסים החיוניים של המדינה. לבסוף על המועצה לוודא כי כל פגיעה בזכות לפרטיות נעשית במידה לפי עקרון המידתיות, לרבות מבחן הפגיעה הפחותה.[173]

12 עתירות שונות הוגשו נגד חוק המודיעין הצרפתי בפני בית הדין האירופי לזכויות אדם בטענה שהחוק אינו עולה בקנה אחד עם המחויבויות של צרפת לפי האמנה האירופית לזכויות אדם וחירויות יסוד. בית הדין איחד את העתירות, אשר בין היתר מעלות טענות בדבר השימוש של גופי המודיעין בצרפת בכלי פצחנות.[174] עתירה זו צפויה להיות הראשונה שבה יידרש בית הדין האירופי לזכויות אדם להידרש במישרין לשאלת אופן החלת סעיף 8 לאמנה בדבר הזכות לפרטיות בהקשר של פעולות פצחנות למטרות ריגול והאזנה.[175]

---

[171] לקריאה נוספת על ה-CNCTR ראו: Asaf Lubin, *"We Only Spy on Foreigners": The Myth of a Universal Right to Privacy and the Practice of Foreign Mass Surveillance*, 18(2) CHICAGO J. INT'L. L. 502, 512, fn. 29 (2018).

[172] ראו: חוק המודיעין, לעיל ה"ש 162, סעיף L.821-5.

[173] שם, בסע' L.801-1, L.833-5.

[174] *Association Confraternelle de la Presse Judiciaire and 11 Other Applications v. France*, , App. No. 49526/15, Eur. Ct. H.R., (2017).

[175] ראו כתב ידיד בית משפט של ארגון Privacy International כחלק מהעתירה, בדגש על הטיעונים המועלים שם בדבר פעולות פצחנות: *Association Confraternelle de la Presse Judiciaire and 11 Other Applications v. France*, App. No. 49526/15, Eur. Ct. H.R., Written Submissions on Behalf Privacy International (Sep. 15, 2017).

3.ג.4. המסגרת החוקית לפעילות פצחנות מודיעינית מצד גופי השיטור

באשר לפעולות פצחנות מצד גופי אכיפה ושיטור, הסמכות עוגנה כחלק מהחוק לחיזוק המאבק בפשיעה המאורגנת, בטרור ובאמצעי המימון שלהם, אשר תיקן את פקודת סדר הדין הפלילי הצרפתית. ככלל, האפשרות להשתמש בפעולת פצחנות מאושרת רק כחלק מחקירות של פשיעה מאורגנת ופשיעה חמורה, לרבות עבירות טרור ועבירות סייבר מסוימות. הדין הצרפתי מכיר בשני מצבים שונים: (1) מתן גישה לחומר מחשב מרחוק וללא ידיעת המשתמש, כאשר הדבר נחוץ למטרות החקירה, ובתוך כדי שימוש ב"מזהה מחשבים" (Computer Identifier);[176] (2) מתן גישה לחומר מחשב מרחוק וללא ידיעת המשתמש, כאשר הדבר נחוץ למטרות החקירה, ובתוך כדי שימוש באמצעי טכנולוגי שמטרתו להשיג גישה למידע השמור במערכת מחשב, או שמוצג על צג מחשבו של משתמש (לרבות מידע שהוקש ומידע שנאסף באמצעות עזרים אודיו-ויזואליים פריפריאליים דוגמת מיקרופונים, מצלמות וסנסורים), לאסוף אותו ולהעבירו.[177] על פי מחקר של הפרלמנט האירופי, אין בדין הצרפתי הסדרה מפורשת של פרוצדורות האיסוף על ידי רשויות אכיפת החוק, לרבות מתודות האגירה והגישה לחומר שנאסף כחלק מפעולות פצחנות. התוצאה היא שבייחוד בכל האמור בהגנה על השרשרת הראייתית, ניכרת מגמה של היעדר אחידות.

---

[176] החוק לחיזוק המאבק בפשיעה המאורגנת, בטרור ובאמצעי המימון שלהם, לעיל ה"ש 163, בסע' 1-95-706 עד 3-95-706. סעיף זה מקביל לאמור בסעיף 41 לכללי סדר הדין הפלילי הפדרליים בארצות הברית, ומוגבל למטרות איכון וזיהוי של מחשבים אנונימיים (בייחוד ככל שהאמור ברשת האפלה). האישור יכול שיינתן לבקשת התובע הכללי בידי השופט לחירויות ומעצרים (le juge des libertés et de la détention) או לחלופין בידי השופט-חוקר. הסדר מיוחד קבוע לפעולות שעניינן שופט, פרלמנטר או עורך דין.

[177] שם, בסע' 1-102-706 עד 2-102-706. סעיף זה מקביל לסמכות השמורה לגופי המודיעין שבחוק המודיעין. גם כאן האישור יכול שיינתן לבקשת התובע הכללי בידי השופט לחירויות ומעצרים או לחלופין בידי השופט-חוקר. בין שזה יהיה התובע הכללי ובין שיהיה השופט-החוקר, ימנו ישות משפטית שתשלים את כל ביצוע הפעולות הטכנולוגיות כחלק מהצו. במקרה הזה, בהינתן שהיעד מזוהה, יורה השופט בצו על העבירה שבגינה אושרו הפעולה, המיקום המדויק והפרטים של מטרת התקיפה ומשך הפעילות המותרת. ככלל, פעולה שאושרה בידי השופט לחירויות ומעצרים מוגבלת לחודש ימים (בכפוף להארכה), ואילו פעולה שאושרה בידי השופט-חוקר מוגבלת לארבעה חודשים (כפוף להארכה). התקופה המרבית לפעילות פצחנות הקבועה בחוק היא שנתיים. השופט מוסמך בכל רגע להפסיק את הפעילות אם ימצא זאת לנכון. ראו שם, בסע' 3-102-706.

[178] עם זאת החוק כן מחייב כי יישמר תיעוד של כל הפעולות שבוצעו כחלק מהשמשת הנוזקה, לרבות הזמן והמועד שבו החלה והסתיימה כל פעולה,[179] ייאסר על שמירת מידע שלא נחוץ למטרות החקירה ומיצוי האמת,[180] וכן כי כל המידע יימחק, ותישמר עדות על המחיקה עם מיצוי ההליכים ולבקשת התובע הכללי.[181]

לבסוף מכוח ההוראה הכללית הפותחת את פקודת סדר הדין הפלילי הצרפתי, Article Préliminaire, חלה על השופטים המאשרים פעולת פצחנות החובה להביא בחשבון את עקרון המידתיות כנגזרת של כבוד האדם.[182] עם זאת על פי חלק מהעדויות, השופטים לרוב אינם מודעים לטכנולוגיה הספציפית שאותה משמישות רשויות החקירה, מטעמי ביטחון שדה ומגבלות ידע טכני, ולכן מתקשים במלאכת האיזון הנדרשת מתפקידם.[183]

3.ד. הדין האיטלקי

3.ד.1. רקע היסטורי

יש תיעוד נרחב של השימוש בנוזקות באיטליה (המכונות "טרויאנים" בשיח היום-יומי האיטלקי) מצד גופי אכיפת החוק כחלק מפעולות פצחנות למטרות חקירות פליליות.[184] למעשה, במחקר שעשה הפרלמנט האירופי נקבע כי השימוש בכלי פצחנות

---

[178] מחקר הפרלמנט האירופי, לעיל ה"ש 108, בעמ' 74.

[179] החוק לחיזוק המאבק בפשיעה המאורגנת, בטרור ובאמצעי המימון שלהם, לעיל ה"ש 163, בסע' 7-102-706.

[180] שם, בסע' 8-102-706.

[181] שם, בסע' 9-102-706.

[182] מחקר הפרלמנט האירופי, לעיל ה"ש 108, בעמ' 75. לשון ההוראה: "The coercive measures to which such a person may be subjected are taken by or under the effective control of judicial authority. They should be strictly limited to the needs of the process, proportionate to the gravity of the offence charged and not such as to infringe human dignity".

[183] שם.

[184] לקריאה נוספת ראו: Carola Frediani, *Intercettazioni col trojan, ecco la proposta di legge*, LA STAMPA (Jan. 31, 2017),

הפך בשנים האחרונות ל"מתודת החקירה המועדפת" על רשויות החקירה האיטלקיות.[185] בתחילה לא ראו בתי המשפט בפעולות מעקב מבוססות-פצחנות פעולות המחייבות הוצאת צו להאזנת סתר.[186] לפיכך פעולות פצחנות אלה לא חייבו הוצאת צו מטעם השופט האמון על החקירה, ודי היה באישורו של התובע הכללי.[187]

עם התפתחות היכולות הטכנולוגיות והשימוש הגובר באמצעי פצחנות חרג בית המשפט העליון האיטלקי (Corte Suprema di Cassazione) מההלכה המקובלת ב-2015 כשפסק כי יש לראות בפעולות פצחנות מצד גופי אכיפת חוק פעולת "מעקב אלקטרוני" המחייבת בהוצאת צו מסורתי לחיפוש ותפיסה.[188] בכך, לראשונה, הוכפפו פעולות פצחנות למסגרת הקבועה בפקודת סדר הדין הפלילי האיטלקי. סעיף 266

---

https://www.lastampa.it/cronaca/2017/01/31/news/intercettazioni-col-trojan-ecco-la-proposta-di-legge-1.34677817 (שם מציינת הכותרת כי חבר הפרלמנט קווינטרלי קבע במסיבת עיתונאים ש"Today these tools are used without a system of guarantees and we do not even know how many people are subjected [to such measures of control]"). עוד ראו: Bill Marczak et. al., *Mapping Hacking Team's "Untraceable" Spyware*, CITIZEN LAB (Feb. 17, 2017), https://citizenlab.ca/2014/02/mapping-hacking-teams-untraceable-spyware/ (שם מצוין כי איטליה היא אחת מהצרכניות הגדולות ביותר של Remote Control System, מערכת מתוחכמת לביצוע תקיפות מחשבים אשר נמכרת לממשלות בלבד מאת החברה האיטלקית Hacking Team.

[185] מחקר הפרלמנט האירופי, לעיל ה"ש 108, בעמ' 59.

[186] ראו לדוגמה: Italian Supreme Court of Cassation, Division V, Decision No. 24695 of October 14, 2009. בעניין זה הכשיר בית המשפט את השימוש בכלי פצחנות לטובת תפיסה והעתקה של חומר מחשב אשר אגור במכשיר המותקף (במקרה הזה הכונן הקשיח של המחשב), אשר שימש את החשוד כחלק מעבודתו. בית המשפט קבע כי חדירה למחשב והעתקה של חומר קיים אינן עולות לכדי חדירה ל"רצף התקשורת", כקבוע בסעיף 266-bis לחוק סדר הדין הפלילי האיטלקי, ועל כן אינם מחייבים בהוצאת צו האזנת סתר. בית המשפט הוסיף כי הנוזקה לכל היותר מקיימת "קשר אופרציונלי" עם המעבד אך זה לא עולה לכדי פעולה האזנה. עם זאת בית המשפט לא עסק בשאלה אם הנוזקה יכולה לשמש גם לפעולות לאיסוף מידע בזמן אמת או לפעילות התקפית (מניפולציה או מחיקה של מידע, הפעלה של פונקציות נוספות על המכשיר וכיו"ב). גישה זו של בית המשפט אומצה בשנית בהליך בעניין Italian Supreme Court of Cassation, Division VI, Bisignani Case, Decision No. 254865 of November 27, 2012. (27 Nov. 2012).

[187] לקריאה נוספת ראו: Giuseppe Vaciago & David Silva Ramalho, *Online Searches and Online Surveillance: the Use of Trojans and Other Types of Malware as Means of Obtaining Evidence in Criminal Proceedings*, 13 DIGITAL EVIDENCE AND ELECTRONIC SIGNATURE LAW REVIEW 88, 91–92 (2016). (להלן: וסיאגו ורמאלו).

[188] ראו: Italian Supreme Court of Cassation, Division VI, Musumeci Case, Decision No. 27100 of May 26, 2015. (26 May 2015).

לפקודה מאפשר "ייעוץ של שיחות או התקשרויות" במסגרת חקירות של רשימת פשעים חמורים המנויה בסעיף. סעיף 266-bis מרחיב את הסמכות לביצוע פעולות מעקב ומתיר גם יירוט של התקשרויות בין מחשבים. עם זאת סעיף 266(2) מחריג פעילות יירוט המבוצעות בבית מגורים או בבית עסק, אלא אם יש חשד כי פעילויות פליליות מתרחשות מתוך המבנה.

בשל הקביעה של בית המשפט העליון האיטלקי ב-2015 כי ניתן להוציא צו תפיסה וחיפוש למטרות פעילות פצחנות התעוררה השאלה כיצד יש ליישב זאת עם החריג המנוי בסעיף 266(2) האוסר על פעילויות מעקב בבתי מגורים ובבתי עסק, שכן פעולות פצחנות מאפשרות מעקב על כל סביבת העבודה של המכשיר המותקף. ב-2016 נדרש בית המשפט העליון האיטלקי לשאלה בשנית. הוא הכיר בעובדה כי הנוזקה עשויה לשמש לפעילויות שונות, לרבות תפיסת כל תקשורת נכנסת ויוצאת מן המכשיר (לרבות היסטורית גלישה, שימוש בדוא"ל, תוכן של שיחות, מיקום גֵאופיזי, הודעות טקסט ותמונות), היכולת להדליק ולכבות אפליקציות שונות על המכשיר, ובייחוד את המצלמה והמיקרופון, ללא ידיעת המשתמש, היכולת לחפש על הכונן הקשיח ולהעתיק את כל המידע השמור ביחידות הזיכרון או חלק, וכן היכולת לפענח כל מה שהוקלד על המכשיר באמצעות הפעלת "רושם הקשות" ואיסוף של כל מה שנצפה על צג המכשיר, ללא קשר לשאלה אם המשתמש הפעיל תוכנות הצפנה ואנונימיזציה.[189]

בשל השימוש הגובר בטכנולוגיה מתקדמת מצד ארגוני פשיעה מאורגנת וארגוני טרור קבע בית המשפט כי יש הצדקה ל"התאמה אפקטיבית" של "החקיקה הקיימת לרבות עקרונות חוקתיים".[190] בית המשפט מבחין בין "חיפוש מקוון" לבין "מעקב מקוון". חיפוש מקוון כרוך רק באיסוף פסיבי של כל המידע שכבר אגור במכשיר, ומעקב מקוון כרוך בכל שאר הפעולות האפשריות מכוח השימוש בנוזקה. בית המשפט בוחר לקרוא קריאה מצמצמת את החריג הקבוע בסעיף 266(2) ומאפשר שימוש בנוזקה גם למטרות מעקב מקוון (אשר ודאי יכלול מעקב אגבי על בית המגורים

---

[189] ראו: Italian Supreme Court of Cassation, Joint Sessions, Scurato Case, Decision No. 26889 of July 1, 2016., Pres. Canzio, Conduct of Case, under "Svolgimento del processo", para. 2 (בית המשפט מציין כי הנוזקה מעורבת ביירוט בזמן אמת של סביבת העבודה של המכשיר המותקף (vera e propria intercettazione ambientale) וממשיך ומונה את השימושים השונים בנוזקה כמתואר לעיל).

[190] שם, בפסקה 10.1.

או בית העסק) אך מצמצם זאת רק לפשעי מאפיה וטרור.[191] לסיכום קובע בית המשפט כי השימוש ב"מיירט דיגיטלי" (captatore informatico) או "חיישן ממוחשב" (sensore del computer) (שמות שונים שבית המשפט נותן לפונקציות של הנוזקה) הם בהלימה הן עם סעיף 266 לפקודת סדר הדין הפלילי האיטלקית, הן עם המשפט החוקתי האיטלקי והן עם חובותיה הבין-לאומיים של איטליה מכוח דיני זכויות האדם (בדגש על סעיף 8 לאמנה האירופית).[192]

אם לא די בתהפוכות האלה, הרי שבמרס 2018 שב בית המשפט העליון האיטלקי לדון בשאלת כלי הפצחנות. עניינו של ההליך בנאשם בשוחד אשר המשטרה השמישה כלי פצחנות כדי להפעיל את הרמקול שבמכשיר הנייד שלו לטובת הקלטת השיחות שקיים. ההקלטות נמשכו גם לאחר סיום החקירה הראשונית וההרשאה השיפוטית. בית המשפט הטיל ספק בשאלה אם במסגרת הנסיבות האמורה, ובייחוד על רקע החריגה האפשרית מסמכות, עלתה פעולת הפצחנות בקנה אחד עם חובותיה הבין-לאומיים של איטליה. בית המשפט העליון החזיר את התיק לבית משפט קמא בבקשה כי יבחן אם פעילות המשטרה עמדה בהוראות החוקה האיטלקית והאמנה האירופית לזכויות אדם.[193]

2.ד.3. הצעות חוק לעיגון הפרקטיקה הנוהגת

בשל התהפוכות בפסיקה הוצעו בשנים האחרונות לא פחות מארבע הצעות שונות מצד חברים שונים בפרלמנט האיטלקי להסדרה מפורשת ומפורטת יותר של

---

[191] שם, בפסקאות 10.1 ו-11.

[192] שם. ראו עוד פסקה 10.2 לפסק הדין. מעניין כי בית המשפט מזכיר בפסקה 6 כי ייתכן שהשופטים המאשרים את הצווים לא יהיו מסוגלים לדעת באפקטיביות ובזמן אמת (בין מכוח ביטחון שדה, בין מכוח מגבלות בידע טכנולוגי ובין מכוח מגבלות פרוצדורליות) מהם השימושים השונים שייעשו בנוזקה (מה שיגרור "אי-יכולת להציע פיקוח מספק על העמידה בדרישות החוק"), אולם בית המשפט לא מצא בטיעון זה בסיס מספק לאיסור גורף על השימוש בנוזקה. ראו שם, בפסקה 6.

[193] לקריאה נוספת על ההליך ראו: Antonella Napolitano, *Italy's Supreme Court decision limits hacking powers and applies safeguards*, PRIVACY INTERNATIONAL (Nov. 2, 2018), https://www.privacyinternational.org/blog/2423/italys-supreme-court-decision-limits-hacking-powers-and-applies-safeguards.

השימוש בכלי פצחנות מצד גופי אכיפת חוק.[194] אף אחת מההצעות האלה לא צלחה את ההתדיינות בפרלמנט. עם זאת ראוי לציין במיוחד את הצעת החוק של Casson והצעת החוק של Quintarelli, שכן שתיהן הבחינו בין השימושים השונים של הנוזקה, כשידוע שפונקציות שונות שלה גוררות עימן רמת פולשנות משתנה. לפיכך הצעות החוק הציעו דרישה לצווים נפרדים לשימושים שונים בנוזקה, חיזוק רמת הפיקוח והבקרה האוחרת, אמצעי ביטחון ופרצודורות למזעור הסיכון לנזק.[195]

כישלון המחוקקים באיטליה להביא להסדרה מפורשת של פעילות פצחנות הובילה את הוועדה לזכויות האדם של האו״ם (בכובעה כמנגנון ביקורת על עמידת איטליה במחויבויותיה לפי האמנה לזכויות אזרחיות ופוליטיות שלה היא צד) לצאת בקריאה נחרצת למדינה להסדיר פעילות זו, במרס 2017.[196] שעה שהוועדה התכנסה בארמון האומות שבז׳נווה, בארמון מאדאמא שברומא מיהרו להקדים תרופה למכה. ב-15 במרס 2017 הצביע הסנאט האיטלקי בעד הצעת חוק שהגיש שר המשפטים האיטלקי אנדראה אורלאנדו שביקשה לבצע רפורמות במערכת הצדק האיטלקית, לרבות באמצעות תיקון לפקודת סדר הדין הפלילי (להלן: חוק אורלאנדו). ב-14 ביוני

---

[194] ראו: וסיאגו ורמאלו, לעיל ה״ש 187, בעמ׳ 92–93 (״In addition to case decisions, during the last year in Italy there has been a succession of four draft laws to bring the investigative tool within the scope of Italian Code of Criminal Procedure: the first draft law was presented as part of a new law on responding to terrorism. In this draft law, a misguided attempt was made to add into Article 266-bis that regulates computer surveillance, the capability of carrying out such type of activity 'also through the use of a tool or software for the remote acquisition of communications and data found in a computer system'. Fortunately, this amendment was criticized by several members of Parliament and by the Prime Minister himself, inasmuch as it introduced the possibility of undertaking utterly invasive activities vis-à-vis citizens without any legal guarantee other than that of viewing such a tool as a mere instance of electronic surveillance. The same fate was met by the 'Greco' Bill of 2 December 2015. At the beginning of 2016, two draft laws were developed ('Casson' amendment and 'Quintarelli' draft law) with a seemingly different approach from the ones of the previous year״).

[195] מחקר הפרלמנט האירופי, לעיל ה״ש 108, בעמ׳ 86–89. לקריאה על הצעת החוק של Quintarelli ראו: Letter by Access Now to Stefano Aterno, Re: Disciplina dell'uso dei captatori legali nel rispetto delle garanzie individuali (29 March 2017), www.civicieinnovatori.it/?page_id=211.

[196] ראו: דוח הוועדה לזכויות האדם של האו״ם בעניין איטליה, לעיל ה״ש 102, בפס׳ 36–37.

אושרה ההצעה גם בבית התחתון. החוק נכנס לתוקפו ב-3 באוגוסט 2017.[197] על פי החוק, הממשלה מתחייבת לגבש חקיקת משנה שתסדיר פעולות פצחנות למטרות חקירה פלילית. החוק מונה שמונה כללים מנחים שמטרתם לקבוע את גבולות המסגרת שלאורם יגבש משרד המשפטים האיטלקי את חקיקת המשנה.[198] אלה הם עיקרי ההסדר:[199] ראשית, הפעלת מיקרופון איננה יכולה להתרחש אוטומטית, והיא מחייבת הפעלה ידנית באישור נפרד של צו בית משפט ובכפוף למגבלות הקבועות באותו הצו; שנית, כל הקלטה של אודיו הנעשית במסגרת הפעלת מיקרופון כאמור מחייבת ברישום ובתיעוד מסודרים כנדרש בסעיף 268 לפקודת סדר הדין הפלילי האיטלקי (הקובע הנחיות בסדר רישום ותיעוד של צווי האזנת סתר), לרבות מועדי תחילת פעולת ההקלטה וסיומה; שלישית, הפעלה של כל פונקצייה במכשיר יכול שתתבצע רק לצורך חקירה של פשעי מאפיה, פשע מאורגן ועבירות טרור, או בבתים פרטיים ובבתי עסק כאשר יש חשש ממשי שעבירות פליליות מתרחשות במקום. בשלב הגשת הבקשה ובשלב אישורה בידי השופט יובהר מדוע פעולת הפצחנות נחוצה למטרות החקירה; רביעית, כל ההקלטות יועברו לשרת מאובטח בשליטת התובע הכללי כדי להגן על השרשרת הראייתית ואת מקוריות הראייה. לאחר סיום פעולת ההקלטה, ובהמלצת גופי החקירה, יש להפסיק את פעולת הנוזקה ולהבטיח כי היא חדלה מלהיות אופרטיבית; חמישית, כל הנוזקות בשימוש גופי אכיפת החוק יהיו כפופות להוראות טכניות שייקבעו בחקיקת משנה. חקיקה זו תעודכן מעת לעת לפי הסטנדרטים המתקדמים ביותר בהקשרי ביטחון, מהימנות ויעילות; שישית, התובע רשאי לאשר פעולות פצחנות בלא צו בית משפט במקרים דחופים. התובע חייב לנמק את הצורך בהוצאת צווי חירום ואת הצורך בפעולת הפצחנות למטרות החקירה. התובע חייב להביא את הצו לידיעת בית המשפט בתוך 48 שעות לטובת קבלת אישורם בדיעבד; שביעית, מידע שנתקבל מפעולת פצחנות בהקשר של פשע ספציפי עשוי לשמש ראיה גם בהקשרן של עבירות חמורות אחרות המנויות בסעיף 380 לפקודת סדר הדין

---

[197] ראו: Legge 23 June 2017, n. 103, G.U. Jul. 4, 2017, N. 154 (It).

[198] לקריאה נוספת ראו: Analysis of the Italian Hacking Reform, under DDL Orlando, PRIVACY INTERNATIONAL (Mar. 5, 2017), https://assets.documentcloud.org/documents/3728074/Privacy-International-s-Analysis-of-the-Italian.pdf.

[199] שם בעמ' 5–6; חוק אורלנדו, לעיל ה"ש 197, בסע' 84(e) תת-סעיפים 1–8.

הפלילי האיטלקי (לדוגמה: עבירת סחר בסמים או גנבה), ובתנאי שהראיה הכרחית (indispensable) להוכחת העבירה. לבסוף, החוק מכיר באפשרות של איסוף מידע אגבי של מי שאינם צד לחקירה כחלק מפעולת הפצחנות. החוק קובע כי במקרה של איסוף אגבי, אין לפרסם ברבים את המידע האגבי שנאסף, לחלוק אותו או לשתף בו. בימים אלה מסיימים במשרד המשפטים האיטלקי את העבודה על חקיקת המשנה כנדרש על פי חוק אורלאנדו. נכון לינואר 2019, טרם פורסמו ברשומות הסדרים נוספים על האמור לעיל. חוק אורלאנדו זכה לביקורת רחבה מצד ארגוני החברה האזרחית, אשר טוענים כי ההסדרים המנויים בו אינם מספקים לשם הבטחת הזכות לפרטיות או שלמות מערכות תקשורת.[200]

בכל האמור בפעולות פצחנות מצד גורמי ביון איטלקיים מחוץ לגבולות איטליה, הדין האיטלקי אינו מסדיר סמכות זאת בחקיקה ראשית.

3.ה. סיכום ביניים

בחינת הדין המשווה מלמדת שמדינות נוספות המתמודדות עם איומי טרור, פשיעה חמורה וריגול נדרשו גם הן כמו ישראל לאסדרה של תחום פעילות הפצחנות. אולם בניגוד להצעות החוק הישראלית, כל אחת מהמדינות הנבחנות אימצה או שהיא בתהליכי אימוץ של הסדרים מורחבים אשר נועדו לשקף איזון בין הנחיצות שבשימוש בכלי הפצחנות למטרות איסוף מודיעין לבין הסיכונים הגלומים בכלי. איזונים אלה כוללים יצירה של מנגנוני ביקורת שיפוטית ומנהלתית, הצרת סמכויות הרשויות בשימוש בכלי התקיפה, הקמת הגנות מסוימות וחסינויות הקבועות בדין ויצירת דרישות פרוצדורליות בתהליך מימוש הבקשה. בפרק החותם נייר זה אדגים כיצד הסדרים שונים הקבועים בדין המשווה במדינות השונות עשויים להיות לישראל מודל שאותו תבקש לחקות בבואה לאמץ חקיקה דומה בישראל.

ד. עקרונות מנחים להסדרה

[200] שם.

בפרק האחרון אני מבקש להציע עקרונות מנחים להסדרה כחלק מעיגון פעולות פצחנות בדין הישראלי. בהתחשב בכך שהצעת החוק המקורית ביקשה להבטיח כי הפרקטיקה תהא תואמת את דיני זכויות האדם ואת אמות המידה המקובלות בתחום זה במשפט הבין-לאומי, מצאתי לנכון להשתמש בשבעת העקרונות המעוגנים בדין הבין-לאומי כבסיס להסדרה. כמו כן אשר לכל עקרון אציין מהן אמות המידה המקובלות, כפי שאלה משתקפות בדין המשווה.

1. עקרון החוקיות

ראוי לברך את ההחלטה להסדיר בחקיקה ראשית את סמכויות השב"כ (ובהקשר זה גם את סמכויות המשטרה) בביצוע פעולות פצחנות. כפי שראינו, בכל המדינות שנבדקו (ואכן זוהי המגמה גם במשפט הבין-לאומי) ניכרת דרישה להסדרה מפורשת ומקיפה של הסמכויות לביצוע פעולות מעקב והאזנה, לרבות פעולות פצחנות.

עם זאת הצעת החוק מבקשת להסדיר פעולות פצחנות של השב"כ בלבד, במנותק מכל הקשר אחר. גישה זו לגיבוש דיני המודיעין הישראליים על דרך של טלאים היא בעייתית ומוגבלת. כפי שמציינים שני וכהנא, "בידי סוכנויות הביון הישראליות מצויות סמכויות מעקב נרחבות, תחת איזונים ובקרות ספורים, ללא מודעות ציבורית – אמנם, ישנה השגחה פרלמנטרית מסוימת, כמו גם ביקורת שיפוטית, אך נראה שרוב הפעילות בתחום נעשית מתחת לרדאר ותוך בקרה מוגבלת".[201] לפיכך מציעים הם כי יש "לבחון מחדש את הדינים הנוגעים למעקב מקוון, במטרה ליצור איזון ראוי יותר בין האינטרס החשוב של ביטחון המדינה לבין זכותם החדשה-ישנה לפרטיות של כל מי שמנהלים את חייהם בעידן הדיגיטלי".[202] חוק האזנת סתר נחקק ב-1979, וחוק המחשבים ב-1995. עם ההתפתחויות הטכנולוגיות, בייחוד בשני העשורים האחרונים, יש מקום לחשיבה מחודשת בדבר

---

[201] יובל שני ועמיר כהנא "מתחת לרדאר: מעקב מקוון בישראל" **המכון הישראלי לדמוקרטיה** 13.3.2017 https://www.idi.org.il//blogs/security-clearance/tracking/14058.

[202] שם.

מארג הדינים המסדיר פעולות ביון ומעקב הן בסדר הדין הפלילי והן מחוצה לו. יש לקוות כי התיקון לחוק השב"כ הוא הסנונית הראשונה המבשרת על בוא האביב ולא יורה ארעי בעוד עונה שחונה.

כך בדין הישראלי חסרים הסדרים רבים הנדרשים בחקיקה ראשית, כגון חוק המעגן את סמכויות המוסד ויחידות אמ"ן (ובהקשר זה את כל הפעילות לאיסוף מודיעין זר (foreign intelligence) בישראל);[203] חוק המסדיר את השימוש בכלי כריית מידע (טכניקות חיפוש וניתוח סטטיסטיים על בסיסי נתוני עתק לרבות על הרשתות החברתיות) ובכלי חיזוי משטרתיים (Predictive Policing) אשר עשויים להתאפיין בפרופיילינג ובהטיות;[204] חקיקת משנה שקופה המסדירה את האופן, המשך והתנאים של אגירת נתוני תקשורת מצד בעלי רישיונות בזק כמו גם את גישתם של גופי אכיפה וביון לאותם הנתונים וגבולות יכולתם בהחזקה ושמירה של נתונים אלה (Bulk Communications Data או BCD);[205] חוק המסדיר את אופן הגישה והיקפה של גופי ביון ואכיפה למאגרי מידע גדולים המוחזקים במשרדי ממשלה, חברות ממשלתיות ופרטיות (לרבות בנקים, חברות תעופה, נמלים ושדות תעופה, בתי מלון, תחבורה ציבורית, בתי חולים, הלשכה המרכזית לסטטיסטיקה, סוכנויות

---

[203] ראו לדוגמה: זאב סגל "למסד את המוסד" **הארץ** 1.3.2010 https://www.haaretz.co.il/opinions/1.1191669; מורן אזולאי "הצעת "חוק השירותים החשאיים": רה"מ עמוס, שר המודיעין יפקח" **Ynet** 22.2.2016 https://www.ynet.co.il/articles/0,7340,L-4769091,00.html (שם טוען ח"כ שלח, מציע הצעת החוק, כי "הסדרת פעולתם של ארגוני המודיעין והפיקוח הממשלתי עליהם הוא מהלך מתבקש, שהיה צריך להתבצע כבר מזמן"); יוסי מלמן "לעגן בחוק את מעמד המוסד" **מעריב** 11.8.2013 https://www.maariv.co.il/news/new.aspx?pn6Vq=11&0r9VQ=EDJLJ. עוד ראו כהנא ושני, לעיל ה"ש 92 (והציטוט המוצא שם).

[204] ראו לדוגמה: אור הירשאוגה והגר שיזף "סיכול ממוקד: השיטה החדשה להתמודדות עם טרור היחידים נחשפת" **הארץ** 26.5.2017 https://www.haaretz.co.il/magazine/.premium-MAGAZINE-1.4124379; עמוס הראל "ישראל עצרה מאות פלסטינים כחשודים בכוונה לבצע פיגועים בגלל פרסומים ברשת" **הארץ** 16.4.2017 https://www.haaretz.co.il/news/politics/.premium-1.4024578; יותם ברגר "המשטרה הסתמכה על תרגום שגוי של פייסבוק ועצרה פלסטיני שכתב 'בוקר טוב'" **הארץ** 22.10.2017 https://www.haaretz.co.il/news/law/.premium-1.4528980.

[205] ראו: כהנא ושני, לעיל ה"ש 68, בעמ' 34–43 וכן 280–281.

נסיעות, רשתות שיווק, חברות אשראי וביטוח) (Bulk Personal Datasets או BPD);[206] חוק המסדיר שימוש משטרתי בטכנולוגיות המדמות תאי סלולר למטרות אכיפה ומעקב (IMSI Catchers/Stingrays);[207] חוק המסדיר אפשרויות גישה ישירה (direct access) לרשתות תקשורת, סמכות אשר על פי כמה מההערכות, מעוגנת בנספחים ביטחוניים חשאיים לרישיונות ספקי אינטרנט וסלולר בישראל;[208] לבסוף, חוק המסדיר שיתופי פעולה מודיעיניים (בין-משרדיים בתוך ישראל ובין גופי ביון ואכיפה ישראליים למקביליהם בעולם).[209]

יתרה מזאת, האיזונים והבלמים הקבועים בחוקים קיימים, דוגמת חוק האזנת סתר וחוק נתוני תקשורת, ראויים גם הם לבחינה מחודשת בראי ההתפתחויות

---

[206] ראו לדוגמה: ברק רביד "ארדן פועל להקמת מאגר מידע על אזרחים ישראלים שתומכים ב-BDS" **הארץ** 21.3.2017 https://www.haaretz.co.il/news/politi/.premium-1.3945031. עוד על הסכנות הטמונות בגישה למאגרי BPD מצד סוכנויות ביון ראו: Owen Bowcott & Richard Norton-Taylor, *UK spy agencies have collected bulk personal data since 1990s, files show*, THE GUARDIAN (Apr. 20, 2016) https://www.theguardian.com/world/2016/apr/21/uk-spy-agencies-collected-bulk-personal-data-since-1990s.

[207] עוד על שימושים בטכנולוגיות אלה למטרות שיטור, שלא בישראל, ראו: יוסי גורביץ "ריגול משטרתי? רק באישור העירייה" **כלכליסט** 22.9.2016 https://www.calcalist.co.il/internet/articles/0,7340,L-3698627,00.html; עוד ראו: Heath Hardman, *The Brave New World of Cell-Site Simulators* (May. 24, 2014) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2440982.

[208] לקריאה נוספת ראו: יובל יועז "האם נספח סודי מאפשר לשב"כ גישה למאגרי המידע של חברות הסלולר?" **הארץ** 23.9.2007 https://www.haaretz.co.il/misc/1.1443629.

[209] ראו לדוגמה: אמיר אורן "מסמך סודי של NSA חושף שיתוף פעולה אמריקאי-ישראלי למעקב מודיעיני במצרים" **הארץ** 4.8.2014 https://www.haaretz.co.il/news/politics/.premium-1.2396477; "מסמך: כך מסייעת ארה"ב ל-8200 במבצעים חשאיים" **וואלה! חדשות** 5.8.2014 https://news.walla.co.il/item/2772714

Memorandum of Understanding Between the National Security Agency/Central Security Service (NSA/CSS) and The Israeli SIGINT National Unit (ISNU) Pertaining to the Protection of U.S. Persons, http://s3.documentcloud.org/documents/785495/doc1.pdf;

לקריאה על הסכנות הטמונות בהיעדר אסדרה של שיתופי פעולה מודיעיניים ראו: HANS BORN & LAN LEIGH, MAKING INTELLIGENCE ACCOUNTABLE: LEGAL STANDARDS AND BEST PRACTICE FOR OVERSIGHT OF INTELLIGENCE AGENCIES 38-59 (2015).

במשפט המשווה והבין-לאומי כמו גם ביכולות הטכנולוגיות של גופי הביון והאכיפה. דגש מיוחד יש לשים על מתודות איסוף שאינן ממוקדות אלא מתאפיינות בשיטות מעקב המונים (mass surveillance) אשר מטבען הן פולשניות יותר ועשויות להוביל לזיהוי חיובי שגוי.

גם אם מלאכת ההסדרה המלאה איננה בת-יישום בשלב זה, לכל הפחות בבואו של המחוקק להתייחס לסוגיית פעולות הפצחנות לא ראוי כי ימקד את כל תשומותיו אך ורק בחוק השב"כ. בהשאלה מהנעשה בדין האנגלי ובדין הצרפתי, יש להציע מסגרת רחבה יותר אשר תחול על פעולות פצחנות בדין הישראלי על כלל הקשריהן החקירתיים (משטרה, מצ"ח, רשות המיסים, רשות ההגירה, שב"כ, אמ"ן, מוסד, מנהלת הסייבר וכיו"ב), כמובן בייחוד על התאמת דיני החיפוש, התפיסה וההמצאה לעידן הדיגיטלי.

הגם שהדין האמריקאי והאיטלקי נעדרים אסדרה מפורשת של פעולות פצחנות מצד גופי ביון, הרי שהדוגמאות באנגלייה ובצרפת מוכיחות שניתן לעגן בחקיקה ראשית אסדרה של פעולות פצחנות למטרות איסוף מודיעין מצד גופי ביון (לרבות מודיעין זר) ואף לספק לציבור מידע נרחב על מתודות איסוף המודיעין של רשויות הביון. כל זאת מבלי לגרום לפגיעה אנושה בביטחון המדינה ובפעילויות הריגול שלה. "קודי ההתנהגות" הנלווים לחוק ה-IPA האנגלי, לדוגמה, הם בשרניים וארכניים וכוללים דוגמאות ממשיות רבות של אופן מימוש החוק. גם הצעת החוק באיטליה כוללת דרישה מפורשת שכל הנוזקות בשימוש גופי אכיפת החוק יהיו כפופות לחקיקת משנה שתעודכן מעת לעת לפי הסטנדרטים המתקדמים ביותר בהקשרי ביטחון ואשר תהיה חשופה לציבור. יש חשיבות רבה, כנגזרת של עקרון החוקיות, כי גם חקיקת המשנה והנהלים בישראל יגיעו לכדי חשיפה לדיון וביקורת ציבורית.[210]

2. עקרונות הנחיצות והפרופורציונליות

[210] לאחרונה גם בארצות הברית החלו לחשוף נהלים פנימיים רבים יותר בעבודת גופי המודיעין, כשמשרד מנהל המודיעין הלאומי פתח אתר אינטרנט, IC On The Record, שבו זמינים עשרות אלפי מסמכים המסדירים את מלאכת העבודה בארגונים השונים ומציגים דיווחים שוטפים שלהם.

הצעת החוק קובעת כמה מאפיינים הראויים לציון בהקשרם של עקרונות הנחיצות והפרופורציונליות. כך לדוגמה קובע החוק כי פעולות פצחנות יוגבלו אך ורק "לפעילות טרור או ריגול שיש בהם משום סיכון חיי אדם או פגיעה חמורה בביטחון המדינה".[211] בכך יש הלימה בין ההצעה לבין הפרקטיקה הגורפת בכל המדינות להגביל את השימוש בכלי פצחנות למספר מצומצם של פשעים חמורים. עוד מעגן החוק את מבחן הפגיעה הפחותה בקובעו כי פעולות פצחנות תאושרנה אך ורק במקרים שבהם "לא ניתן, באופן סביר, להשיג את המטרה האמורה בדרך אחרת".[212]

עם זאת הקושי המרכזי בהצעת החוק נעוץ בבקשה להעתיק ההסדרים הקבועים בחוק האזנת סתר לפעולות פצחנות. לכאורה מדובר ביישום של תזכיר חוק סדר הדין הפלילי (סמכויות אכיפה – המצאה, חיפוש, כניסה ותפיסה), התשע"א–2011, שם טענו המציעים:

> "חדירה לחומר מחשב ללא ידיעת המחזיק וללא נוכחות עדים מהווה אמצע חקירתי שפגיעתו בזכויות מוגנות, של הנחפש ושל צדדים שלישיים, רבה. עם זאת יהיו נסיבות בהן אין מנוס מביצוע חיפוש סמוי כאמור וזאת בין היתר בנסיבות שבהן הודעה ונוכחות של המחזיק בעת ביצוע החיפוש יביאו לשיבוב הראיה או מחיקתה, או בנסיבות שבהן עצם ידיעתו של המחזיק בחומר המחשב על ביצוע החיפוש יביא לסיכול החקירה נגדו. מוצע לקבוע כי שימוש באמצעי זה יתאפשר במקרים מיוחדים בלבד, בהם אין אפשרות להשיג את מטרות החקירה באמצעים פוגעניים פחות. החדירה לחומר המחשב יכול שתהיה נקודתית ויכול שתהיה מתמשכת. בנסיבות חריגות אלה, מוצע לאפשר בצו שיפוטי ביצוע החיפוש ללא ידיעת המחזיק. נוכח הדמיון הקיים בין חדירה סמויה כאמור לחומר מחשב לבין האזנת סתר, אף שאין מדובר בקליטה של מידע העובר בתקשורת בין מחשבים, מוצע להחיל את כל ההוראות הקבועות בפרקים ג' ו-ד' לחוק

---

[211] הצעת חוק המאבק בטרור, 1492–1494.

[212] היה עדיף הנוסח המעוגן בתזכיר חוק סדר הדין הפלילי, לעיל ה"ש 72, בסע' 65, הקובע כי בטרם אישור צו לביצוע פעולות בחומר מחשב על בית המשפט לשקול "האם ניתן להשיג את מטרת הפעולה בדרך שפגיעתה באדם או בפרטיותו תהא פחותה".

האזנת סתר כך שיראו סמכות זו כהאזנת סתר, ויחולו עליה הוראות חוק האזנת סתר״.[213]

מבחינה זו התיקון לחוק השב״כ וכן תזכיר החוק מבקשים להחיל את חוק האזנת סתר על כל משמעויותיו גם על פעולות פצחנות. ודאי שמנקודת המבט של המציעים זה נראה מהלך מתבקש, שכן הוא עדיף על ההסדר הקיים (קרי פעולות פצחנות בהסדרה מינימלית מכוח הפקודה).[214] אני מסכים שבבחירה בין שתי חלופות גרועות, מוטב לבחור בזו הגרועה פחות. עם זאת ראוי לשאול אם האיזונים הקבועים בחוק מ-1979 עודם משקפים הסדר ראוי ב-2018, הן בהקשר של האזנות סתר ובוודאי בהקשר של פעולות פצחנות. כפי שנידון בהרחבה לעיל, פעולות פצחנות אינן ככל פעילות מעקב אחרת. האתגרים הביטחוניים הייחודיים הקשורים בשימוש בכלי פצחנות, לצד הפולשנות הייחודית הנוגעת לחדירה לחומר מחשב,[215] מחייבים מלאכת איזונים שונה ורגישות יתרה לסכנות הכרוכות בשימוש בכלי פצחנות. לפיכך פעולות פצחנות ראויות להסדר מחמיר יותר, מעין ״חוק האזנת סתר פלוס״. בהקשר הזה החוק אינו מנחה את ראש הממשלה, כמי שממונה על אישור פעולות פצחנות, לבחינת רשימה סגורה של שיקולים ואינטרסים ייחודיים בבואו לדון בדרישות הנחיצות והמידתיות של הפעולה. רשימה שכזו קיימת הן בדין האנגלי והן בדין הצרפתי. עוד החוק אינו מאשרר את מבחן המידתיות במובן הצר, הגם שייתכן שזה יחול מכוח חוק-יסוד: כבוד האדם וחירותו. בהקשר הזה יודגש כי הדין האנגלי מאמץ את מבחני המידתיות כבלם מרכזי בתהליך הביקורת השיפוטית מפני הסיכון לשימוש שרירותי בכלי

---

[213] שם, בעמ׳ 41.

[214] כזכור זוהי גם עמדתה של אהרוני-גולדנברג, וראו לעיל ה״ש 78 (לרבות הטקסט הנלווה).

[215] ראוי לשוב ולהדגיש נקודה זו. כך לדוגמה דבריה של השופטת נילי ארד, שהדגישה כי המחשב מכיל ממד אישי של המשתמש בו, שכן ״חולש על מרחב המחיה המוחשי והמטאפיסי של המשתמש״. היא מדגישה עוד כי פעילות במחשב עולה לכדי ״עדות ממקור ראשון, ושותפות למצבים ולאירועים בעלי חשיבות אישית ואינטימית בהליכות חיינו. באמצעות טכנולוגיות המידע העומדות לרשות המשתמש במחשב, יכול ויישמר במרחב הווירטואלי הפרטי שלו, עולמו האישי, המסחרי והיצירתי, על מכלול התכתבויותיו הפרטיות והעסקיות, הגיגיו, עניינים הנוגעים לעבודתו, ולמחוזות פעילותו, ומראי המקום וההיסטוריה של גלישותיו.. המאפשר בניית פרופיל של המשתמש, המגדיר את עולמו על אישיותו תחביביו ושאיפותיו, כמו גם את מערכות היחסים והתקשורת שלו במהלך חייו ופעילותו במסגרת העבודה, המשפחה, הקהילה, ההתקשרות הבינלאומית וכל כיוצ״ב״. ראו: ע״ע (ארצי) 90/08 **טלי איסקוב ענבר נ׳ מדינת ישראל – הממונה על חוק עבודת נשים**, בפס׳ 6 (פורסם בנבו 8.2.2011).

הפצחנות המודיעניים. לצד זאת אחת הביקורות המרכזיות על הדין בארצות הברית היא שהוא נעדר את מבחני הנחיצות, בייחוד בכל האמור במניעת אבחון חיובי שגוי. אחזור לנקודות אלה בהרחבה רבה יותר בתת-סעיף 3 שעניינו האישור המקדים.

3. עקרון האישור המקדים

קיים קושי רעיוני במדינה שומרת חוק לאישור פעולות מעקב ללא ביקורת שיפוטית קודם לאישור. הדבר נכון שבעתיים בפעולות פולשניות ובעלת פוטנציאל נזק גבוה, דוגמת פעולות פצחנות. מתן הסמכות לראש הממשלה לאשר בעצמו, וללא צו, פעולות שכאלה (ובחירום מתן הסמכות לראש השירות לאשר הפעולות לבדו, אגב דיווח אוחר ליועץ המשפטי לממשלה) אינו עולה בקנה אחד עם המגמה בעולם. בכל המדינות שנבדקו, ולפי הסטנדרטים המקובלים בדיני זכויות האדם הבין-לאומיים, מעורבות של גורם שיפוטי בתהליך האישור של פעולות מעקב, בוודאי פעולות פצחנות, היא הכרחית. גישה זאת מוצאת ביטוי גם במחקר של הפרלמנט האירופי (שבחן את דיני הפצחנות גם בגרמניה, בהולנד, בפולין ובאוסטרליה):

> "All countries require *ex-ante* judicial authorization for police hacking, demonstrating the seriousness of the privacy infringement. Legislation does acknowledge that urgent or exigent circumsntaces may sometimes demand that the receipt of prior authorization is not necessary; however, Member States still require that judicial authorization is subsequantely obtained"[216]

[216] מחקר הפרלמנט האירופי, לעיל ה"ש 108, בעמ' 49.

יתרה מזאת, הצעת החוק לא דנה לעומקה בסד השיקולים שצריכים להנחות את הרשות החוקרת בהגשת הבקשה לצו או את הגוף המאשר במועד אישור הבקשה. ניתן לשוב לתזכיר חוק סדר הדין הפלילי (סמכויות אכיפה – המצאה, חיפוש, כניסה ותפיסה) משנת 2011. ככלל מדגיש התזכיר כי "שני עקרונות מנחים עומדים בבסיס קביעת השיקולים המהותיים המוצעים שעל בית המשפט לשקול בבואו לתת את הצווים הנוגעים לפעולות בחומר מחשב: (א) הצורך בעידוד ביקורת שיפוטית אקטיבית ומעמיקה של הבקשה המוגשת על ידי רשויות האכיפה, תוך הכוונה לשקילת כל השיקולים הרלוונטיים להחלטה אם להיענות לבקשת הצו המבוקש אם לאו; (ב) הצורך בגמישות ההסדר החקיקתי, נוכח מציאות טכנולוגית דינאמית המשתנה באופן מתמיד". מקובלות עליי הבחנות אלה, וישכיל המחוקק אם יביא אותן בחשבון בבואו לגבש את סד השיקולים הרלוונטי לפעולות פצחנות.[217]

לפי האמור לעיל, סעיף 65(ב) לתזכיר מונה כמה וכמה שיקולים שעל בית המשפט לשקול בבואו לאשר צו לביצוע פעולות בחומר מחשב:

> "(1) המטרה שלשמה מתבקש הצו לביצוע הפעולה בחומר המחשב; (2) חומרת העבירה, שלצורך חקירתה מתבקש הצו לרבות נסיבות ביצועה וזהות החשוד; (3) פעולות החקירה שבוצעו עד כה; (4) מידת הפגיעה בפרטיות או בזכויות אחרות הצפויה כתוצאה מהחדירה לחומר המחשב, בשים לב לאלו: (א) מיקומו של המחשב, השימוש בו וסוג המידע האגור בו; (ב) סוג הפעולה בחומר מחשב המבוקש, אופן ביצועה והאם השלבים בביצוע הפעולה ניתנם לתכנון וידועים מראש; (ג) אפשרות כי החומר יישמר ולא ישובש גם ללא ביצוע הפעולה בחומר המחשב על פי הצו; (ד) האם המחזיק בחומר המחשב לגביו מתבקש הצו – הוא חשוד; אם אינו חשוד – טיב היחסים שבינו לבין החשוד, לרבות האם הוא ספק שירות; (ה) מידת הפגיעה בפרטיותם או בזכויות אחרות של אחרים כתוצאה מביצוע הפעולה, לרבות האם הפעולה מתייחסת לאדם מזוהה או לאדם

[217] ראו: תזכיר חוק סדר הדין הפלילי, לעיל ה"ש 72, בעמ' 32.

שזיהויו אינו ידוע או אינו ודאי; (ו) יכולת תיעוד הפעולה לצרכי בקרה של הפעולות המבוקשות על פי הצו ועמידה בתנאים לביצועה".[218]

לא זו אף זו, סעיף 65(ג) מונה סדרי עדיפויות שנועדו להנחות עוד את בית המשפט במועד אישור הצו. בהקשר זה מדגיש הסעיף כי יש עדיפות לפעולה גלויה על פני פעולה סמויה, עדיפות לפעולה בחומר אגור על פני פעולה בחומר שעתיד להתקבל או להיווצר ועדיפות לעיון בחלק מחומר מחשב ולא בכל חומר המחשב.[219]

שיקולים אלה מהווים כר פורה לתחילת דיון באשר לנוסח הראוי להסדרת פעולות פצחנות בדין הישראלי. על אלה מבקש אני להוסיף עוד ארבע נקודות לבחינה ועיון: ראשית, יש להדגיש במיוחד את הזכות לאנונימיות ברשת ואת הפעלת אמצעי ההצפנה מצד משתמשים, בייחוד בכל האמור בפעילות ברשת האפלה. הצעת החוק אינה מתייחסת כלל לטכנולוגיות מסוג אלה ואינה מסדירה את גבולות המותר והאסור בניסיונות גופי החקירה לעקוף את אותן טכנולוגיות כחלק מחקירתם. יתרה מזאת, בהקשר של פעולות ברשת האפלה, ובהמשך לדיון שהתעורר בארצות הברית, יש מקום לדון בהיקף סמכות השיפוט של שופטים לאשר בצו פעולות פצחנות אשר השלכותיהן עשויות להיות מורגשות מחוץ לגבולות המדינה.[220]

שנית, יש לשים דגש מיוחד על מתודת ההתפשטות ולחייב מפורשות את הרשות החוקרת להסביר כיצד היא מתכוונת להחדיר את הנוזקה למחשבו של המשתמש או המשתמשים הספציפיים. מתודות התפשטות שונות גוזרות פגיעה משתנה בפרטיות

---

[218] היה עדיף הנוסח המעוגן בתזכיר חוק סדר הדין הפלילי, שם, בסע' 65(ב), הקובע כי בטרם אישור צו לביצוע פעולות בחומר מחשב על בית המשפט לשקול "האם ניתן להשיג את מטרת הפעולה בדרך שפגיעתה באדם או בפרטיותו תהא פחותה".

[219] שם, בעמ' 35. התזכיר מדגיש עוד כי לעיתים דווקא צו הנוגע לחומר אגור יכול להיות בעל פגיעה חמורה מזו שבצו לחומר עתידי, "שהרי לעיתים חיפוש בחומר מחשב אגור יכול להיות פוגעני יותר אם מדובר בהיקף גדול או שמדובר בחומר רגיש". התזכיר עוד מציע רעיון מעניין של צו שמירה (המקביל לצו הקפאת שימוש בחפץ) אשר עשוי להיות בעל פגיעה מוגבלת יותר בזכות לפרטיות, שכן אינו מאפשר בשלב הוצאתו לרשויות האכיפה להיחשף לתוכן המידע שנשמר עד להוצאת צו המצאה נפרד.

[220] בהקשר הזה יש להדגיש במיוחד את שטחי יהודה ושומרון ורצועת עזה ואת פעילות השב"כ בשטחים המצויים בתפיסה לוחמתית. לא ברור כלל מהדין אם הזכות לפרטיות המעוגנת בחוק-יסוד: כבוד האדם וחירותו חלה על התושבים הפלסטינים בשטחים אלה, כמו גם גבולות סמכות השיפוט וההגבלות על פעילות הפצחנות של השב"כ בהקשר זה. עוד בהקשר זה ראו: ליאב אורגד "חוקה של מי ועבור מי? על היקף התחולה של חוקי היסוד" **משפט וממשל** יב, 145 (התשע"ע).

וסיכון משתנה לשלמות מערכי התקשורת ומהימנותם. בהקשר הזה יובהר כי החוק איננו מדגיש כלל את החשש מאיסוף של "מידע אגבי", כשהחוק מתיר חדירה למחשביהם של מי שאינם חשודים כלל (לרבות על דרך של חדירה לקבוצה גדולה של מחשבים בעלי מאפיינים דומים מכוח צו נפח).

שלישית, הצעת החוק אינה מבהירה את גבולותיו של צו בודד לאישור פעולת פצחנות.[221] יש מקום לדרוש מפורשות כי פעולות שונות באמצעות הנוזקה, קרי שימוש במטע"דים שונים, יחייבו צווים שונים או בקשות חוזרות לשינויים בצו קיים. כך לדוגמה אין דין זיהויו של מחשב באמצעות תוכנה מאכנת כדין רוגלה למטרות איסוף מידע האגור על כוננו הקשיח. אין דין הרוגלה כדין הפעלת "רושם הקשות" על מחשבו של איש. אין דין "רושם ההקשות" כדין הפעלה של מצלמה או מיקרופון בזמן אמת לאיסוף מידע על סביבתו של המשתמש. לפיכך על הגורם המאשר להיות מעורב בכל שלבי השימוש בנוזקה ולא לקבל דיווח רק בדיעבד על פעילויותיה השונות, בייחוד בהקשרן של פעולות התקפיות שאינן פסיביות ואיסוף מידע בזמן אמת.[222] בהקשר הזה יש חשיבות רבה בהבהרה כי לא ייעשה שימוש בכלי פצחנות לשום מטרה אחרת שאיננה מטרת איסוף מודיעין (קרי פעילות אקטיבית, התקפית) אלא במקרי חירום (דוגמת "פצצה מתקתקת"), וגם זאת באישור נפרד של בית המשפט.

רביעית, יש ביקורת חוזרת על ששופטים אינם ממלאים עבודתם נאמנה ואינם מבקרים כדבעי בקשות של המשטרה לצווי חיפוש,[223] לרבות צווי האזנת סתר.[224] ראוי כי כל הסדרה של התחום תהיה תלויה בחיזוק הביקורת השיפוטית על אישור פעולות פצחנות, בין היתר על דרך של העצמת כישוריהם הטכנולוגיים של השופטים ויכולתם

---

[221] כאמור, החוק מתיר ביצוע "פעולה במחשב או בחומר מחשב" כל עוד היא חיונית לשם סיכול או מניעה של פעילות טרור או ריגול. החוק אפוא אינו מצמצם את סוגי הפעולות שניתן לבצע בחומר המחשב כמו את היקף ההיתר (למשל אם השב"כ רשאי לאסוף מידע לפי החוק על אזרחים תמימים וחפים מפשע ככלי לגיוס סוכנים ומודיעים).

[222] גם הפרלמנט האירופי הדגיש כי המגמה היא הבחנה בין צווים שונים לפונקציות שונות של הנוזקה וראו: מחקר הפרלמנט האירופי, לעיל ה"ש 108, בעמ' 51.

[223] ראו: ששי גז ומשה רונן, **המשפט הפלילי**, עמ' 43 (2001).

[224] ראו: יואב יצחק "חשיפה: המשטרה ביקשה 1773 האזנות סתר; נשיאי בתי המשפט סירבו לארבע בקשות בלבד" **News1** 18.11.2001 https://www.news1.co.il/Archive/001-D-3962-00.html; "חותמת גומי? 99% מהבקשות להאזנות סתר אושרו" **Ynet** 28.6.2010 https://www.ynet.co.il/articles/0,7340,L-3911150,00.html.

להתמודד עם השאלות הטכניות הניצבות לפתחם. גם האפשרות להיוועץ עם מומחי טכנולוגיה וזכויות דיגיטליות שאינם מטעם המדינה יכולה להיות רלוונטית. בהקשר הזה יש מקום לבחון אם בדומה להסדרים הקיימים בדין האמריקאי, האנגלי והצרפתי, וכן לפי המנגנונים הקבועים בהצעת החוק הקיימת באיטליה, יש מקום להקים ישות נפרדת ועצמאית בתוך הרשות השופטת, בעלת שופטים מומחים בעלי רקע קודם רלוונטי, אשר יאשרו פעולות לצרכים מודיעיניים.[225] בכך תקום יכולתם של שופטים להתמודד עם האתגר הטכנולוגי-מודיעיני הכרוך בהבנה לאשורם של הצרכים הטכניים של גופי אכיפת החוק לצד הסיכונים שבשימוש בכלי פצחנות לביטחון מערכי התקשורת שלנו.

4. עקרון אמצעי הביטחון

הצעת החוק בנוסחה הקיים אינה מציעה את הערובות המינימליות הדרושות כדי לאפשר לאדם להתגונן מפני הפגיעה בזכויותיו ולמזער נזקים פוטנציאליים לצדדים שלישיים. בהקשר הזה ראוי להתעכב על כמה נקודות מרכזיות.

ראשית, הצעת החוק אינה קובעת דבר על ההבחנה שבין תקיפות ממוקדות לתקיפות רוחב של מספר רב של מחשבים מכוח צו בודד. ייתכנו מצבים שיצדיקו תקיפות רחבות יותר, ועל החוק לקבוע מסגרות כדי להגביל פעולות שכאלה רק למידה הנחוצה. יש להבטיח צמצום במספר המחשבים המותקפים וכן נהלים ברורים באשר למחיקת מידע שאיננו רלוונטי.[226]

יתרה מזאת, הצעת החוק אינה מדגישה את שרשרת המשמורת הראייתית ואינה קובעת תניות מיוחדות הנוגעות למאפיינים הספציפיים של חומר מחשב בכל האמור בתיעוד פעולת הפצחנות ואגירת המידע שנאסף מהפעולה. בניגוד גמור לזה, תזכיר החוק מתייחס במישרין ל"נדיפותה של הראיה האלקטרונית, שמטבע הדברים עלולה להימחק או להשתנות באופן שלא ניתן יהיה לשחזרה בדיעבד".[227] על החוק לקבוע חובות תיעוד לרבות הוראות מיוחדות בנוגע לדוח החדירה לחומר המחשב

[225] להרחבה ראו: כהנא ושני, לעיל ה"ש 68, בעמ' 281–292.
[226] ראו: מחקר הפרלמנט האירופי, לעיל ה"ש 108, בעמ' 50.
[227] ראו: תזכיר חוק סדר הדין הפלילי, לעיל ה"ש 72, בעמ' 31.

שיושלם במהלך פעולת הפצחנות,[228] הסדרים מיוחדים הנוגעים לפיצוח צפנים או פריצה של מנגנוני אבטחה על מנת לאתר את חומר המחשב הרלוונטי וכן חובות באשר לרמת מקצועיותו של החוקר (״בעל מקצוע מיומן״, כהגדרתו בפקודת סדר הדין הפלילי).[229] עוד חסר בהצעת החוק הסדרים מכוח דרישות ה-Weber 6 בייחוד בכל האמור למשך זמן האגירה של מידע שנאסף מפעולות פצחנות, מגבלות על הגישה למידע ועל אופי שמירתו, הגופים שרשאים לקבל גישה למידע וכן דרישות בנוגע למחיקת המידע עם סיום החקירה.

עוד ראוי להדגיש כי הצעת החוק אינה נותנת את הדין לשאלת השימוש הראייתי בחומר שנאסף. דגש מיוחד יש לשים על סעיף 74 לחוק סדר הדין הפלילי המקים את החובה לאפשר עיון בחומר החקירה לנאשם. עולה השאלה אם הרשות החוקרת תידרש להתייחס לטכניקות ששימשו אותה לביצוע החיפוש כבר בשלב התיעוד ובדוח החקירה, או שמא רק במהלך המשפט. ראוי לתהות מהן ההשלכות של גילוי שכזה על אפקטיביות השימוש בטכניקות חקירתיות אלה בעתיד. על המחוקק לקבוע איזון נכון בין האינטרס של הנאשם לדעת אילו אמצעים חקירתיים השמישו נגדו, לאינטרס של הרשות החוקרת לשמור על סודיות אמצעי החקירה שלה.

החוק גם נעדר התייחסות לשאלת האגירה של חולשות, ובייחוד חולשות אפס ימים, כבסיס לקידום פעולות פצחנות. יש מקום לבחון בדין הישראלי אימוץ של מנגנון ״פרוצדורת נכסי חולשה״ (VEP) הקיים בדין האמריקאי והאנגלי ואת השיקולים המנחים את המנגנונים הללו (כפי שמתואר בנספח 3 למאמר זה). על ישראל להיות שקופה בעניין קיומו של מנגנון וזה ומאפייניו. כמו כן יש להסדיר בחקיקת משנה כל רכש של טכנולוגיות תקיפת מחשבים שלא בפיתוח עצמאי (off-the-shelf) ושל חולשות אפס מים.

5. עקרונות השקיפות, הבקרה, היידוע והשיפוי

[228] לעניין דוח החדירה לחומר מחשב, ראו: שם, בסע׳ 86.
[229] ראו: קוזלובסקי, לעיל ה״ש 73, בעמ׳ 74 וההפניות שם.

ד"ר ביטון טוען במאמרו "במשפט אנו בוטחים" כי ישראל נעדרת מנגנונים מוסדיים לביקורת ופיקוח על גופי הביון והמודיעין שלה, ושמה את מבטחה בעיקרו בבתי המשפט וביועצים המשפטים.[230] כפי שכבר ראינו, מעת לעת מתעוררת השאלה אם בתי המשפט והיועצים מספקים די פיקוח ומעודדים די שקיפות כדי להבטיח עמידה בדרישות של מנהל תקין והגנה על חירויות יסוד. שני וכהנא לדוגמה גורסים כי יש לחזק את הבקרה המוסדית ואף מציעים את המודל של "מינוי נציב עצמאי להגנת מידע", אשר יחזיק ב"סיווג הביטחוני הנדרש על מנת לבחון את הסדרי החקיקה, ההנחיות הפנימיות ואת המדיניות הכללית הנוגעת למעקב מקוון".[231] באפשרותו של נציב כזה, למשל, להתייחס לתלונות על שימוש לרעה בסמכויות רשויות הביטחון. בהקשר הזה ראוי להזכיר את הדיון דלעיל, בייחוד בדין האנגלי והצרפתי, באשר למקצועיות גופי הביקורת ויכולתם המוגבלת בהבנת הטכנולוגיה המורכבת הכרוכה בפעולות פצחנות וכן באשר להיקף יכולתם להפנים חומרי מודיעין ולזהות את צורכי הקהילייה. על נציב שכזה, אם יועסק, יהיה להיות בעל הרקע המתאים ולהסתייע בצוות מומחים מייעץ בעלי ניסיון הן בצד הטכנולוגי והן בצד של זכויות אדם וחירויות יסוד.

יתרה מזאת, כדי שיוגשו תלונות, על המתלונן לדעת כי הוא היה יעד לפעולת פצחנות. בהקשר הזה מדגישים שני וכהנא את החשיבות שבפיתוח "זכות להודעה על מעקב, שמכוחה – במקרים בהם יתאפשר, לאחר מעשה – ידווח לאזרחים כי נעשה שימוש [במידע שלהם] על-ידי רשות ביטחון". מיותר לציין כי הצעת החוק הישראלית

---

[230] ראו: Raphael Bitton, *In Law We Trust: The Israeli Case of Overseeing Intelligence*, in GLOBAL INTELLIGENCE OVERSIGHT 141 (Goldman & Rascoff eds., 2016).

[231] ראו: שני וכהנא, לעיל ה"ש 201. במקום אחר מציעים כהנא ושני כי "יש להקים גוף פיקוח עצמאי לבקרה על פעילות המעקב המקוון השוטפת שלרשויות המדינה, לבחינת הציות להוראות שבצווים, וכן לייעוץ ולהנחייה מקצועית בנוגע להיבטי הגנת פרטיות באסדרה רלוונטית. חלופה להקמת גוף זה היא הרחבת סמכויותיה של הרשות להגנה על הפרטיות (לשעבר רמו"ט), כך שיוקנו לה סמכויות לפקח על הגנת הפרטיות בפעילויות מעקב מקוון של רשויות הביטחון ואכיפת החוק. עוד חלופה היא ייסוד פונקציה של אומבודסמן לענייני פרטיות במעקב מקוון - גוף עצמאי, נטול פניות, בעל סמכויות ריאקטיביות לחקור תלונות, למצוא באופן בלתי פורמלי פתרונות להן, ולעתים לתת פומבי לממצאיו, תוך שמירת הדיסקרטיות של המתלוננים". וראו: כהנא ושני, לעיל ה"ש 68, בעמ' 290.

אינה קובעת כל נוהל נוסף בדבר מנגנוני בקרה, חובות יידוע או זכאות לפיצוי בהקשר של פעולות פצחנות.[232]

יש מקום לשקול מתיחת פנים גם כשמדובר בחובות הדיווח התקופתיות הקיימות על פעולות מעקב בדין הישראלי (בין לראש הממשלה, בין לוועדת החוקה, חוק ומשפט, בין לוועדת חוץ וביטחון או ליועץ המשפטי לממשלה). יש צורך לצקת תוכן ממשי לחובות דיווח אלה ולהגדיר בחוק אילו פרטים יש לכלול בדיווחים, וכן לדאוג כי פרטי הדוח (לכל הפחות מידע סטטיסטי, גם אם לא מידע פרטני) יהיו חשופים לעיון הציבור ולביקורת ציבורית.[233]

ה. סיכום

מעת לעת משמיעים מנכ"לים של חברות טכנולוגיה וספקיות שירות אינטרנטיות תחזיות עגומות בדבר עתיד הזכות לפרטיות.[234] פרופ' בירנהק השכיל לתאר את סכנת ההכחדה העומדת לפתחה של הזכות בעידן הדיגיטלי:

> "בשונה משאר הזכויות, הפרטיות נתונה תחת מתקפה קשה שמאיימת להכריעה. בעידן דיגיטלי שמציע טכנולוגיות של מעקב, בתוספת לחץ ביטחוני עצום מצד המדינה ובמיוחד אחרי אירועי האחד עשר בספטמבר 2001, ובתוספת לחצי השוק התובע יתר-יעילות, הזכות לפרטיות נאבקת על מקומה ונדמה לפעמים שהמאבק להגנתה הוא מלחמת מאסף... מקור האיום הקלאסי הוא המדינה וכיום, גורם משמעותי נוסף שמאיים על

---

[232] להשוואה לדין הזר בהקשרים אלו, ראו מחקר הפרלמנט האירופי, לעיל ה"ש 108, בעמ' 52–54.

[233] להרחבה ראו כהנא ושני, לעיל ה"ש 68, בעמ' 291–292.

[234] ראו: Bobbie Johnson, *Privacy No Longer Social Norm, Says Facebook Founder*, THE GUARDIAN (Jan. 10, 2010) https://www.theguardian.com/technology/2010/jan/11/facebook-privacy; Polly Sprenger, *SUN On Privacy: 'Get Over It'*, WIRED (Jan. 26, 1999) https://www.wired.com/1999/01/sun-on-privacy-get-over-it/.

> הפרטיות בא מצד השוק. כמובן האיום האולטימטיבי הוא שיתוף הפעולה שבין המדינה לשוק״.[235]

השימוש בכלי פצחנות מציב אתגר נוסף לזכות לפרטיות, ולצד זאת הוא מציב גם אתגר לשלמות מערכי התקשורת שכולנו תלויים בהם בניהול שגרת חיינו. למול אתגרים אלה התיקון המוצע לחוק השב״כ, כמו גם הצעת חוק סדר הדין הפלילי (סמכויות אכיפה – המצאה, חיפוש, כניסה ותפיסה), אינם נותנים מענה מספק. הצעת החוק לוקה בכמה וכמה כשלים בעיגון הסטנדרטים המקובלים בדין המשווה ובדין הבין-לאומי ואינה מספקת הגנות ראויות בראי הרגישויות הייחודיות שבשימוש בכלים התקפיים ממרחב הסייבר. היכולת חסרת התקדים של גופי אכיפת החוק להשתמש בכלים אלה כדי להשיג שליטה הרמטית על כל מסגרות הפעילות של אדם, די בה כדי לעורר שדים דיסטופיים קמאיים המחייבים אסדרה מקיפה בהרבה.

יש לראות בחקר המקרה של פצחנות מצד גופי אכיפת החוק מיקרוקוסמוס למסגרת הדינים הקיימת בישראל בדבר אסדרה של מעקב מקוון. עמדו על כך כהנא ושני מהמכון הישראלי לדמוקרטיה כשהדגישו שהדין הישראלי ״סובל מתת-אסדרה בשורת סוגיות שהדין המשווה נותן להם מענה״.[236] לצד זאת כללים חשאיים, היעדר שקיפות וביקורת שיפוטית מוגבלת מייצרים מסגרת נורמטיבית בעייתית אשר אינה עולה בקנה אחד עם דרישות חברת מידע דמוקרטית במאה העשרים ואחת.

הניסיון של המחוקק לייצר אסדרה של תחום הפצחנות פירושה חקיקה בטלאים אשר חוטאת לעיקר. הסדרת השימוש בכלי מעקב מקוון למטרות ריגול ואכיפת חוק חשובה מאין כמוה ומחייבת בחינה עדינה של מלאכת האיזונים הקיימת והתאמתה לעידן החדש. יש לקוות כי הדיונים בוועדת החוקה, חוק ומשפט סביב התיקון לחוק השב״כ יהוו פתח לדיון רחב בהרבה מצד הכנסת סביב רפורמה כוללת של תחום זה בדין הישראלי. תקוותי כי מאמר זה ישמש לחברי הכנסת בבחינת מורה נבוכים בבואם להתמודד עם האתגר החקיקתי האדיר שלפניהם.

---

[235] מיכאל בירנהק ״שליטה והסכמה: הבסיס העיוני של הזכות לפרטיות״ **משפט וממשל** יא 9, 10, 14 (2007).

[236] ראו: כהנא ושני, לעיל ה״ש 68, בעמ׳ 10.

ו. נספחים

1. מודל PrEP[237]

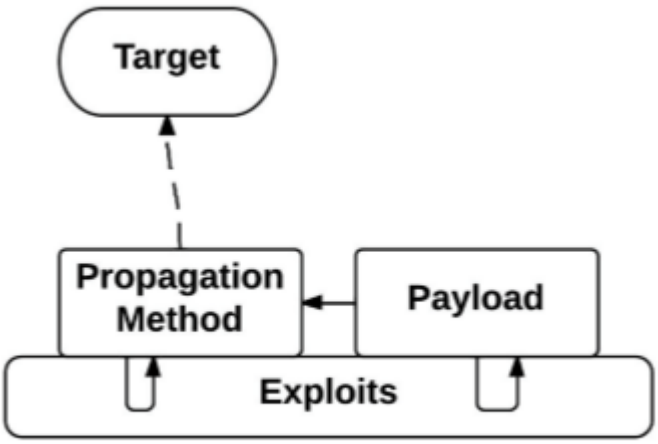


Figure 1: PrEP Framework

[237] ראו: טריי הר, לעיל ה"ש 48, בעמ' 87.

2. התגלגלות מערך רובורשת[238]

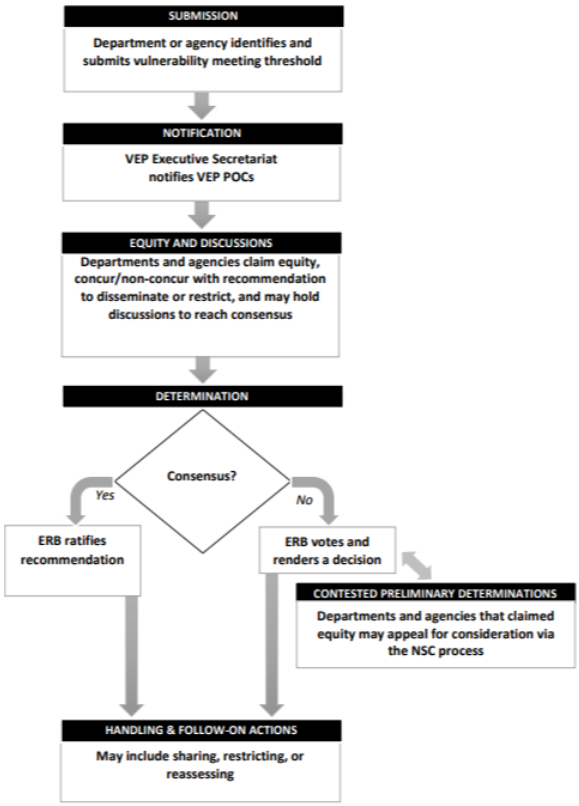
תרשים 1: **המחשה לפעולה של תוכנה זדונית**

מקור: אתר האינטרנט של האף.בי.איי בעיבוד משרד מבקר המדינה.

[238] ראו: מבקר המדינה **דו"ח שנתי 67ב**, לעיל ה"ש 91, 1861.

3. מנגנון "פרוצדורת נכסי חולשה" (VEP) האמריקאי והאנגלי והשיקולים המנחים את המנגנון[239]

המנגנון האמריקאי-



[239] ראו: *Vulnerabilities Equities Policy and Process for the United States Government*, THE WHITE HOUSE (Nov. 15, 2017), https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF. עוד ראו: פרוצדורת נכסי חולשה – אנגליה, לעיל ה"ש 160.

Part I – Defense Equity Considerations

1.A. Threat Considerations

- Where is the product used? How widely is it used?
- How broad is the range of products or versions affected?
- Are threat actors likely to exploit this vulnerability, if it were known to them?

1.B. Vulnerability Considerations

- What access must a threat actor possess to exploit this vulnerability?
- Is exploitation of this vulnerability alone sufficient to cause harm?
- How likely is it that threat actors will discover or acquire knowledge of this vulnerability

1.C. Impact Considerations

- How much do users rely on the security of the product?
- How severe is the vulnerability? What are the potential consequences of exploitation of this vulnerability?
- What access or benefit does a threat actor gain by exploiting this vulnerability?
- What is the likelihood that adversaries will reverse engineer a patch, discover the vulnerability and use it against unpatched systems?
- Will enough USG information systems, U.S. businesses and/or consumers actually install the patch to offset the harm to security caused by educating attackers about the vulnerability?

1.D. Migration Considerations

- Can the product be configured to mitigate this vulnerability? Do other mechanisms exist to mitigate the risks from this vulnerability?
- Are impacts of this vulnerability mitigated by existing best-practice guidance, standard configurations, or security practices?

- If the vulnerability is disclosed, how likely is it that the vendor or another entity will develop and release a patch or update that effectively mitigates it?
- If a patch or update is released, how likely is it to be applied to vulnerable systems? How soon? What percentage of vulnerable systems will remain forever unpatched or unpatched for more than a year after the patch is released?
- Can exploitation of this vulnerability by threat actors be detected by USG or other members of the defensive community?

Part 2 – Intelligence, Law Enforcement, and Operational Equity Considerations

2.A. Operational Value Considerations

- Can this vulnerability be exploited to support intelligence collection, cyber operations, or law enforcement evidence collection?
- What is the demonstrated value of this vulnerability for intelligence collection, cyber operations, and/or law enforcement evidence collection?
- What is its potential (future) value?
- What is the operational effectiveness of this vulnerability?

2.B. Operational Impact Considerations

- Does exploitation of this vulnerability provide specialized operational value against cyber threat actors or their operations? Against high-priority National Intelligence Priorities Framework (NIPF) or military targets? For protection of warfighters or civilians?
- Do alternative means exist to realize the operational benefits of exploiting this vulnerability?
- Would disclosing this vulnerability reveal any intelligence sources or methods?

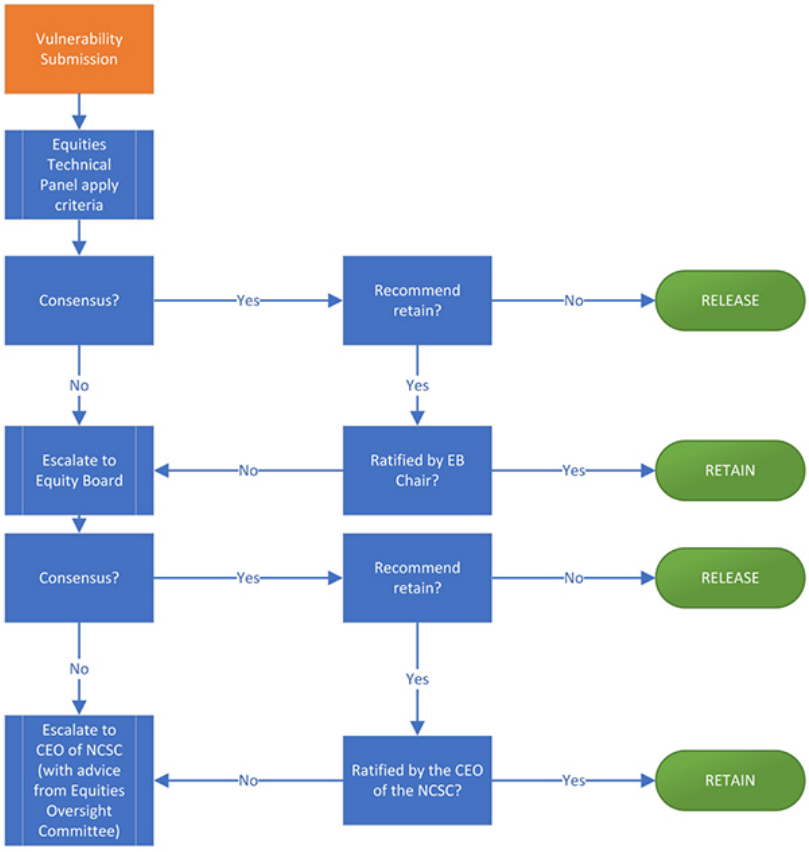
Part 3 – Commercial Equity Considerations

- If USG knowledge of this vulnerability were to be revealed, what risks could that pose for USG relationships with industry?

Part 4 – International Partnership Equity Considerations

- If USG knowledge of this vulnerability were to be revealed, what risks could that pose for USG international relations?

המנגנון האנגלי-



Decision criteria

In reaching a decision on whether to release or retain a vulnerability, the following broad criteria are considered:

Possible remediation. Consideration of the possible routes to mitigate the impact of the vulnerability, in particular focusing on whether there is a viable route to release, or whether releasing it would have a negative impact on national security.

Operational necessity. Consideration of the intelligence value to the UK in retaining the vulnerability, which includes the following questions:

- What operational value can be gained from this capability?
- What are the intelligence opportunities from this capability?
- How reliant are we on this vulnerability to realise intelligence?
- How likely is a disclosure to impact other operational capabilities or partners?

Defensive risk. An assessment of the impact on security of not releasing the vulnerability in the context of the UK and its allies, including Government departments, critical national infrastructure, companies and private citizens. This includes:

- How likely is it that this vulnerability is/could be discovered by someone else?
- How likely is it that this vulnerability could be exploited by someone else?
- What technology/sector is exposed if left unpatched?
- What is the potential damage if the vulnerability is exploited?
- Without a patch applied to the software are other mitigation opportunities possible such as configuration changes?

The criteria above will be applied to determine whether there is a clear and overriding national security benefit in retaining a vulnerability. These are broad criteria and they are not all relevant in every case. Equally, individual

vulnerabilities may give rise to particular considerations which are relevant to the decision. Assessment in relation to a number of these factors is based on standardised criteria and past experience, including applying the use of the Common Vulnerability Scoring System where appropriate.

Exceptions

There are certain limited circumstances where vulnerabilities may not be subject to the Equities Process. These include vulnerabilities that have already been subjected to similar considerations by a partner and shared with us.

A second example, is where the software in question is no longer supported by the vendor: were a vulnerability to be discovered in such software, there would be no route by which it could be patched.

Another circumstance is where a software vendor has made a design choice which is inherently vulnerable, but which they have clearly documented, or alternatively where a system owner has made a similarly vulnerable configuration or architectural choice. These vulnerabilities can be categorised as "vulnerable-by-design", and there is no security benefit in fixing a single vulnerability in inherently vulnerable software.